Administrar Platform Services Controller

Actualización 2

Modificado el 02 de mayo de 2022

VMware vSphere 6.7

VMware ESXi 6.7

vCenter Server 6.7



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de *Administrar Platform Services Controller* 7

Información actualizada 9

1 Introducción a Platform Services Controller 11

Tipos de implementación de vCenter Server y Platform Services Controller 11

Topologías de implementación con instancias de Platform Services Controller externas y alta disponibilidad 15

Comprender los sitios, los nombres de dominio y los dominios de vSphere 18

Capacidades de Platform Services Controller 19

Administrar servicios de Platform Services Controller 20

Servicios de Platform Services Controller 20

Administrar servicios de Platform Services Controller desde vSphere Client 22

Administrar servicios de Platform Services Controller desde vSphere Web Client 23

Usar scripts para administrar servicios de Platform Services Controller 23

Administración del dispositivo de Platform Services Controller 25

Administrar el dispositivo con la interfaz de administración de dispositivos virtuales de Platform Services Controller 25

Administrar el dispositivo desde su propio shell 26

Agregar un dispositivo de Platform Services Controller a un dominio de Active Directory 26

2 Autenticar vSphere con vCenter Single Sign-On 28

Descripción general de vCenter Single Sign-On 29

Cómo vCenter Single Sign-On protege el entorno 29

Componentes de vCenter Single Sign-On 32

Cómo influye vCenter Single Sign-On en la instalación 33

Usar vCenter Single Sign-On con vSphere 33

Grupos del dominio de vCenter Single Sign-On 36

Configurar orígenes de identidad de vCenter Single Sign-On 37

Orígenes de identidad para vCenter Server con vCenter Single Sign-On 38

Establecer el dominio predeterminado de vCenter Single Sign-On 39

Agregar o editar un origen de identidad vCenter Single Sign-On 40

Configurar orígenes de identidad de Active Directory 42

Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory 44

Usar vCenter Single Sign-On con autenticación de sesión de Windows 46

Descripción de la autenticación de dos factores de vCenter Server 46

Inicio de sesión de autenticación de tarjeta inteligente 47

Configurar y usar la autenticación de tarjeta inteligente 48
Configurar el proxy inverso para solicitar certificados de clientes 49
Usar la línea de comandos para administrar la autenticación de tarjeta inteligente 50
Administrar la autenticación de tarjeta inteligente 55
Configurar directivas de revocación para autenticación de tarjeta inteligente 57
Configurar la autenticación de RSA SecurID 59
Administrar el mensaje de inicio de sesión 62
Utilizar vCenter Single Sign-On como el proveedor de identidad para otro proveedor de servicios 63
Unirse a un proveedor de servicios SAML a la federación de identidades 64
Servicio de token de seguridad (STS) 65
Actualizar el certificado del servicio de token de seguridad 65
Generar un nuevo certificado de firma de STS en el dispositivo 67
Generar un nuevo certificado de firma de STS en una instalación de Windows de vCenter 69
Determinar la fecha de caducidad de un certificado SSL de LDAPS 70
Administrar directivas de vCenter Single Sign-On 71
Editar la directiva de contraseñas de vCenter Single Sign-On 71
Editar la directiva de bloqueo de vCenter Single Sign-On 72
Editar la directiva de tokens de vCenter Single Sign-On 73
Editar la notificación de caducidad de la contraseña para usuarios de Active Directory 74
Administrar usuarios y grupos de vCenter Single Sign-On 76
Agregar usuarios de vCenter Single Sign-On 77
Deshabilitar y habilitar usuarios de vCenter Single Sign-On 78
Eliminar un usuario de vCenter Single Sign-On 79
Editar un usuario de vCenter Single Sign-On 80
Agregar un grupo de vCenter Single Sign-On 81
Agregar miembros a un grupo de vCenter Single Sign-On 81
Quitar miembros de un grupo de vCenter Single Sign-On 82
Eliminar usuarios de solución vCenter Single Sign-On 83
Cambiar la contraseña de vCenter Single Sign-On 84
Prácticas recomendadas de seguridad de vCenter Single Sign-On 84

3 Certificados de seguridad de vSphere 86
Requisitos de certificados para distintas rutas de acceso de la solución 88
Descripción general de la administración de certificados 92
Descripción general del reemplazo de certificados 95
Casos en que vSphere utiliza certificados 98
Servicios básicos de identidad de VMware y VMCA 101
Descripción general de VMware Endpoint Certificate Store 101
Administrar la revocación de certificados 104
Reemplazar certificados en implementaciones de gran tamaño 104

Administrar certificados con vSphere Client 106

Explorar los almacenes de certificados desde vSphere Client 108

Establecer el umbral para las advertencias de caducidad de certificados de vCenter 108

Reemplazar certificados por nuevos certificados firmados por VMCA desde vSphere Client 109

Configurar el sistema para utilizar certificados personalizados desde Platform Services Controller 111

Generar una solicitud de firma del certificado para el certificado SSL de máquina con vSphere Client (certificados personalizados) 111

Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados) 112

Agregar un certificado raíz de confianza al almacén de certificados 113

Agregar certificados personalizados desde Platform Services Controller 114

Administrar certificados desde vSphere Web Client 116

Ver certificados de vCenter con vSphere Web Client 116

Administrar certificados con la utilidad vSphere Certificate Manager 117

Opciones de Certificate Manager y flujos de trabajo en este documento 118

Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados 120

Convertir a VMCA en una entidad de certificación intermedia (Certificate Manager) 122

Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia) 123

Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados 125

Reemplazar un certificado SSL de máquina por un certificado de VMCA (entidad de certificación intermedia) 126

Reemplazar certificados de usuario de solución por certificados de VMCA (entidad de certificación intermedia) 128

Reemplazar todos los certificados por certificados personalizados (Certificate Manager) 128

Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados) 130

Reemplazar un certificado SSL de máquina por un certificado personalizado 131

Reemplazar los certificados de usuarios de soluciones con certificados personalizados 132

Revertir la última operación realizada volviendo a publicar certificados antiguos 134

Restablecer todos los certificados 134

Reemplazar certificados de forma manual 134

Información sobre la interrupción y el inicio de servicios 134

Reemplazar certificados firmados por VMCA existentes por certificados firmados por VMCA nuevos 135

Generar un nuevo certificado raíz firmado por VMCA 136

Reemplazar certificados SSL de máquina por certificados firmados por VMCA 138

Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA 142

Reemplazar el certificado de VMware Directory Service en entornos de modo mixto 149

Utilizar VMCA como entidad de certificación intermedia 150

Reemplazar el certificado raíz (entidad de certificación intermedia) 151
Reemplazar certificados SSL de máquina (entidad de certificación intermedia) 154
Reemplazar certificados de usuarios de solución (entidad de certificación intermedia) 157
Reemplazar el certificado de VMware Directory Service en entornos de modo mixto 164
Usar certificados personalizados con vSphere 165
Solicitar certificados e importar un certificado raíz personalizado 166
Reemplazar certificados SSL de máquina por certificados personalizados 168
Reemplazar los certificados de usuarios de soluciones con certificados personalizados 170
Reemplazar el certificado de VMware Directory Service en entornos de modo mixto 172

4 Administrar servicios y certificados con comandos de CLI 173
Privilegios necesarios para ejecutar CLI 174
Cambiar las opciones de configuración de certool 175
Referencia de comandos de inicialización de certool 176
Referencia de comandos de administración de certool 180
Referencia de comandos vecs-cli 182
Referencia de comando dir-cli 189

5 Solucionar problemas en Platform Services Controller 198
Determinar la causa de un error de Lookup Service 198
No se puede iniciar sesión con la autenticación del dominio de Active Directory 199
Se produce un error en el inicio de sesión en vCenter Server porque la cuenta de usuario está bloqueada 201
La replicación de VMware Directory Service puede tardar mucho 202
Exportar un paquete de soporte de Platform Services Controller 203
Referencia a registros del servicio Platform Services Controller 203

Acerca de *Administrar Platform Services Controller*

En la documentación de *Administrar Platform Services Controller*, se explica de qué manera VMware® Platform Services Controller™ se adapta al entorno de vSphere para ayudarlo a realizar tareas comunes, como la administración de certificados y la configuración de vCenter Single Sign-On.

En *Administrar Platform Services Controller*, se explica cómo se puede configurar la autenticación con vCenter Single Sign-On y cómo se pueden administrar certificados para vCenter Server y los servicios relacionados.

Tabla 1-1. Información destacada de *Administrar Platform Services Controller*

Temas	Contenido destacado
Introducción a Platform Services Controller	■ Modelos de implementación de vCenter Server y Platform Services Controller. NOTA: Esta información se modifica en cada versión del producto. ■ Servicios de Platform Services Controller en Linux y Windows. ■ Administración de servicios de Platform Services Controller. ■ Administración de un dispositivo de Platform Services Controller mediante VAMI.
Autenticar vSphere con vCenter Single Sign-On	■ Arquitectura del proceso de autenticación. ■ Forma de agregar orígenes de identidad para que los usuarios del dominio se puedan autenticar. ■ Autenticación de dos factores. ■ Administración de usuarios, grupos y directivas.
Certificados de seguridad de vSphere	■ Modelo de certificado y opciones de reemplazo de certificados. ■ Reemplazo de certificados desde la interfaz de usuario (casos simples). ■ Reemplazo de certificados mediante la utilidad Certificate Manager. ■ Reemplazo de certificados mediante la CLI (situaciones complejas). ■ Referencia de la CLI para la administración de certificados.

Documentación relacionada

En un documento complementario, *Seguridad de vSphere*, se describen las medidas y las características de seguridad disponibles que se pueden llevar a cabo para proteger el entorno frente a ataques. En ese documento también se explica cómo se configuran los permisos y se incluye una referencia a los privilegios.

Además de estos documentos, VMware publica la *guía de configuración de seguridad de vSphere* (anteriormente denominada la *guía de fortalecimiento*) para cada versión de vSphere. Puede obtener dicha guía en http://www.vmware.com/security/hardening-guides.html. La *guía de configuración de seguridad de vSphere* contiene directrices de configuración de seguridad que el cliente puede o debe definir, así como la configuración de seguridad proporcionada por VMware que el cliente debe auditar para garantizar que aún tiene el valor predeterminado.

Audiencia prevista

Esta información está dirigida a administradores que desean configurar Platform Services Controller y los servicios asociados. La información está escrita para administradores del sistema expertos en Windows y Linux que están familiarizados con la tecnología de máquina virtual y las operaciones de centro de datos.

vSphere Client y vSphere Web Client

Las instrucciones de esta guía reflejan vSphere Client (GUI basada en HTML5). También puede utilizar las instrucciones para realizar las tareas mediante vSphere Web Client (GUI basada en Flex).

Las tareas para las que el flujo de trabajo difiere significativamente entre vSphere Client y vSphere Web Client tienen procedimientos duplicados que proporcionan los pasos de acuerdo con la interfaz del cliente correspondiente. Los procedimientos que se relacionan con vSphere Web Client, contienen vSphere Web Client en el título.

Nota En vSphere 6.7 Update 1, casi todas las funcionalidades de vSphere Web Client se implementan en vSphere Client. Para obtener una lista actualizada del resto de las funcionalidades no compatibles, consulte Actualizaciones de funcionalidades para vSphere Client.

Información actualizada

Este documento sobre *Administrar Platform Services Controller* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de la documentación sobre *Administrar Platform Services Controller*.

Revisión	Descripción
02 MAYO DE 2022	■ Se corrigió un error ortográfico en Cómo vCenter Single Sign-On protege el entorno. ■ Actualización menor a Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory. ■ Actualización menor a Generar un nuevo certificado de firma de STS en el dispositivo. ■ Se corrigieron los pasos en Determinar la fecha de caducidad de un certificado SSL de LDAPS. ■ Actualización menor a Requisitos de certificados para distintas rutas de acceso de la solución. ■ Actualización menor a Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados.
08 de octubre de 2021	■ Se eliminó el no rechazo como requisito de certificado de la documentación. ■ Actualización menor a Servicios de Platform Services Controller. ■ Se actualizaron las descripciones del nombre de usuario y la URL del servidor principal en Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory. ■ Se solucionó un problema con el guion de `-securIDAuthn` en Configurar la autenticación de RSA SecurID. Cuando se copiaba el comando, no se ejecutaba correctamente. ■ Se corrigió un error tipográfico en Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados. ■ Actualización menor a Información sobre la interrupción y el inicio de servicios. ■ Se corrigió un error tipográfico en Reemplazar certificados SSL de máquina por certificados firmados por VMCA. ■ Se corrigió un error tipográfico en Referencia de comando dir-cli.
12 de agosto de 2020	En VMware, valoramos la inclusión. Para fomentar este principio entre nuestros clientes, nuestros partners y nuestra comunidad interna, estamos reemplazando parte de la terminología en nuestro contenido. Hemos actualizado esta guía para eliminar el lenguaje no inclusivo.

Revisión	Descripción
11 de MAYO de 2020	■ Se agregó información sobre el DN base para los usuarios y el DN base para los grupos que van a Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory. ■ Se agregó la ubicación de los registros en vCenter Server para que Windows Referencia a registros del servicio Platform Services Controller. ■ Actualización menor a Solicitar certificados e importar un certificado raíz personalizado. ■ Se actualizó el Referencia de comandos de inicialización de certool para utilizar la opción `--gencsr` en lugar de `--initcsr`. ■ Se actualizó Reemplazar certificados de usuarios de solución (entidad de certificación intermedia) para mostrar que el almacén de certificados de vpxd existe solo en el vCenter Server Appliance. ■ Se agregó información sobre el ID de evento 2889 a Configurar orígenes de identidad de Active Directory.
26 de agosto de 2019	■ Se corrigió la ubicación del archivo `certool.cfg` en Cambiar las opciones de configuración de certool. ■ Se actualizó la información sobre el uso del atributo userPrincipalName en Configurar la autenticación de RSA SecurID.
11 de abril de 2019	Versión inicial.

Introducción a Platform Services Controller

1

Platform Services Controller ofrece servicios de infraestructura comunes para el entorno de vSphere. Entre estos servicios, se encuentran la concesión de licencias, la administración de certificados y la autenticación con vCenter Single Sign-On.



Mejoras en la interfaz de Platform Services Controller (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_qcyuyhrt/uiConfId/49694343/)

Este capítulo incluye los siguientes temas:

- Tipos de implementación de vCenter Server y Platform Services Controller
- Topologías de implementación con instancias de Platform Services Controller externas y alta disponibilidad
- Comprender los sitios, los nombres de dominio y los dominios de vSphere
- Capacidades de Platform Services Controller
- Administrar servicios de Platform Services Controller
- Administración del dispositivo de Platform Services Controller

Tipos de implementación de vCenter Server y Platform Services Controller

Puede implementar vCenter Server Appliance o instalar vCenter Server para Windows con una instancia de Platform Services Controller integrada o externa. También puede implementar Platform Services Controller como dispositivo o instalarlo en Windows. Si es necesario, puede usar un entorno de sistema operativo mixto.

Antes de implementar vCenter Server Appliance o instalar vCenter Server para Windows, debe determinar el modelo de implementación que sea adecuado para su entorno. Para cada implementación o instalación, debe seleccionar uno de los tres tipos de implementación.

Tabla 1-1. Tipos de implementación de vCenter Server y Platform Services Controller

Tipo de implementación	Descripción
vCenter Server con una instancia de Platform Services Controller integrada	Todos los servicios que se incluyen en el paquete con Platform Services Controller se implementan junto con los servicios de vCenter Server en la misma máquina virtual o el mismo servidor físico.
Platform Services Controller	Solo los servicios que se incluyen en el paquete con Platform Services Controller se implementan en la máquina virtual o el servidor físico.
vCenter Server con una instancia de Platform Services Controller externa (Requiere una instancia de Platform Services Controller externa)	Solo los servicios de vCenter Server se implementan en la máquina virtual o el servidor físico. Debe registrar dicha instancia de vCenter Server con una instancia de Platform Services Controller que haya implementado o instalado anteriormente.

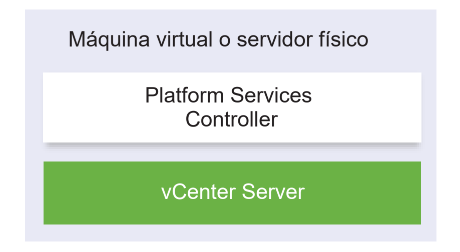
Nota Las implementaciones de vCenter Server que utilizan una instancia externa de Platform Services Controller no se admitirán en versiones futuras de vSphere. Implemente o actualice a una implementación de vCenter Server mediante una instancia integrada de Platform Services Controller. Para obtener más información, consulte el artículo http://kb.vmware.com/kb/60229 de la base de conocimientos de VMware.

vCenter Server con una instancia de Platform Services Controller integrada

El uso de una instancia integrada de Platform Services Controller da como resultado una implementación independiente que tiene su propio dominio de vCenter Single Sign-On con un único sitio.

A partir de vSphere 6.5 Update 2, otras instancias de vCenter Server con una instancia de Platform Services Controller integrada pueden combinarse para habilitar Enhanced Linked Mode.

Figura 1-1. vCenter Server con una instancia de Platform Services Controller integrada



La instalación de vCenter Server con una instancia integrada de Platform Services Controller posee las siguientes ventajas:

- La conexión entre vCenter Server y Platform Services Controller no se realiza a través de la red, y vCenter Server no está propenso a interrupciones causadas por problemas de conectividad y resolución de nombres entre vCenter Server y Platform Services Controller.

- Si instala vCenter Server en máquinas virtuales o servidores físicos con Windows, necesita menos licencias de Windows.
- Debe administrar menos máquinas virtuales o servidores físicos.

Puede configurar vCenter Server Appliance con una instancia de Platform Services Controller integrada en la configuración de alta disponibilidad de vCenter. Para obtener información, consulte *Disponibilidad de vSphere*.

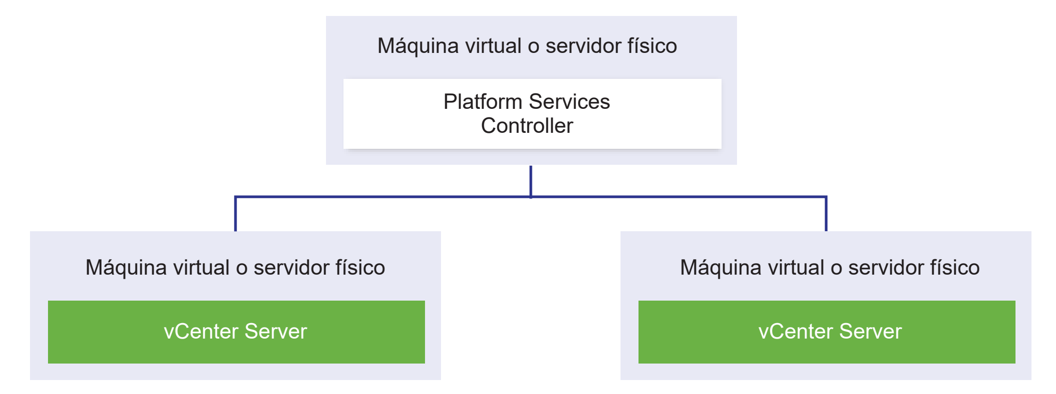
Platform Services Controller y vCenter Server con una instancia de Platform Services Controller externa

Cuando implementa o instala una instancia de Platform Services Controller, puede crear un dominio de vCenter Single Sign-On o unirse a un dominio de vCenter Single Sign-On existente. Las instancias de Platform Services Controller que se unieron replican sus datos de infraestructura, como la información de autenticación y licencias, y puede abarcar varios sitios de vCenter Single Sign-On. Para obtener información, consulte Comprender los sitios, los nombres de dominio y los dominios de vSphere.

Nota Las implementaciones de vCenter Server que utilizan una instancia externa de Platform Services Controller no se admitirán en versiones futuras de vSphere. Implemente o actualice a una implementación de vCenter Server mediante una instancia integrada de Platform Services Controller. Para obtener más información, consulte el artículo http://kb.vmware.com/kb/60229 de la base de conocimientos de VMware.

Puede registrar varias instancias de vCenter Server con una instancia común externa de Platform Services Controller. Las instancias de vCenter Server asumen el sitio de vCenter Single Sign-On de la instancia de Platform Services Controller con la que están registradas. Todas las instancias de vCenter Server que están registradas con una instancia común o con diferentes instancias unidas de Platform Services Controller se conectan en el modo Enhanced Linked Mode.

Figura 1-2. Ejemplo de dos instancias de vCenter Server con una instancia común externa de Platform Services Controller



La instalación de vCenter Server con una instancia externa de Platform Services Controller posee las siguientes desventajas:

- La conexión entre vCenter Server y Platform Services Controller puede tener problemas de conectividad y de resolución de nombres.
- Si instala vCenter Server en máquinas virtuales o servidores físicos con Windows, necesitará más licencias de Microsoft Windows.
- Deberá administrar más máquinas virtuales o servidores físicos.

Para obtener información sobre los máximos de Platform Services Controller y vCenter Server, consulte la documentación de *Máximos de configuración*.

Para obtener información sobre cómo configurar vCenter Server Appliance con una instancia externa de Platform Services Controller en la configuración de alta disponibilidad de vCenter, consulte *Disponibilidad de vSphere*.

Nota Después de implementar o instalar vCenter Server con una instancia externa de Platform Services Controller, puede volver a configurar el tipo de implementación y cambiar a vCenter Server con una instancia integrada de Platform Services Controller.

Entorno de sistema operativo mixto

Una instancia de vCenter Server instalada en Windows puede registrarse con una instancia de Platform Services Controller instalada en Windows o un dispositivo de Platform Services Controller. Una instancia de vCenter Server Appliance puede registrarse con una instancia de Platform Services Controller instalada en Windows o con un dispositivo de Platform Services Controller. Tanto vCenter Server como vCenter Server Appliance pueden registrarse con la misma instancia de Platform Services Controller.

Figura 1-3. Ejemplo de un entorno de sistema operativo mixto con una instancia de Platform Services Controller externa en Windows

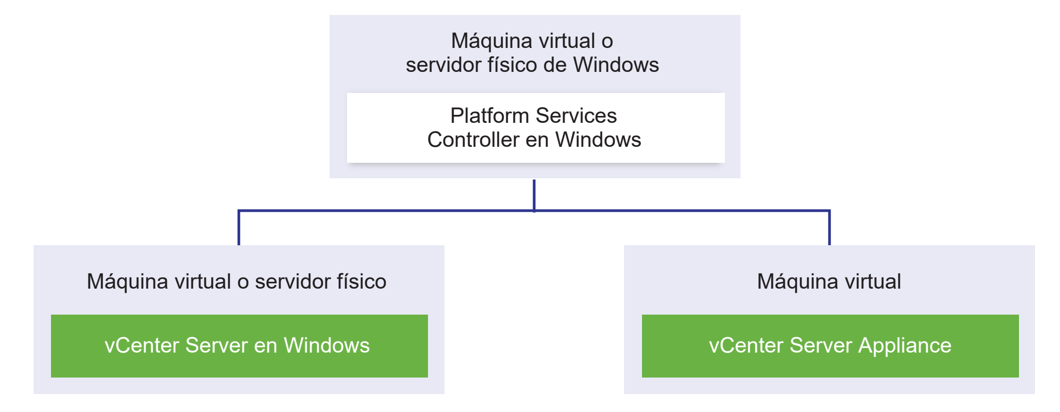
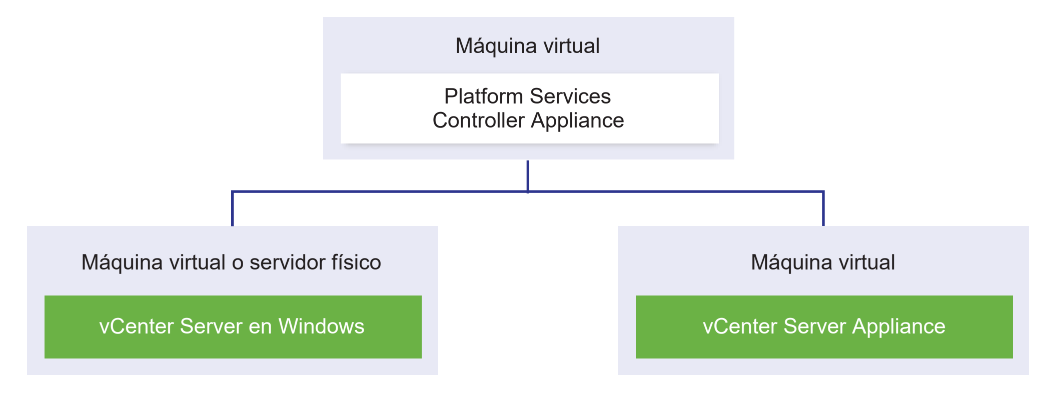


Figura 1-4. Ejemplo de un entorno de sistema operativo mixto con una aplicación de Platform Services Controller externa



Nota Para garantizar la capacidad de administración y mantenimiento, use solamente dispositivos o instalaciones para Windows de vCenter Server y Platform Services Controller.

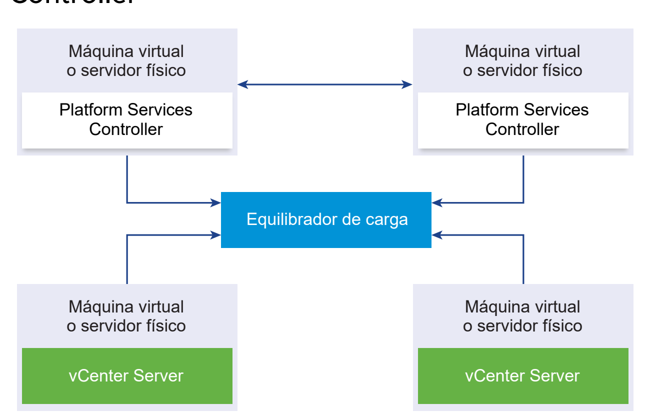
Topologías de implementación con instancias de Platform Services Controller externas y alta disponibilidad

Para garantizar la alta disponibilidad de Platform Services Controller en las implementaciones externas, es necesario instalar o implementar al menos dos instancias unidas de Platform Services Controller en el dominio de vCenter Single Sign-On. Si se utiliza un equilibrador de carga de terceros, es posible garantizar una conmutación por error automática sin tiempo de inactividad.

Nota Las implementaciones de vCenter Server que utilizan una instancia externa de Platform Services Controller no se admitirán en versiones futuras de vSphere. Implemente o actualice a una implementación de vCenter Server mediante una instancia integrada de Platform Services Controller. Para obtener más información, consulte el artículo de la base de conocimientos KB 60229.

Platform Services Controller con un equilibrador de carga

Figura 1-5. Ejemplo de un par con carga equilibrada de instancias de Platform Services Controller



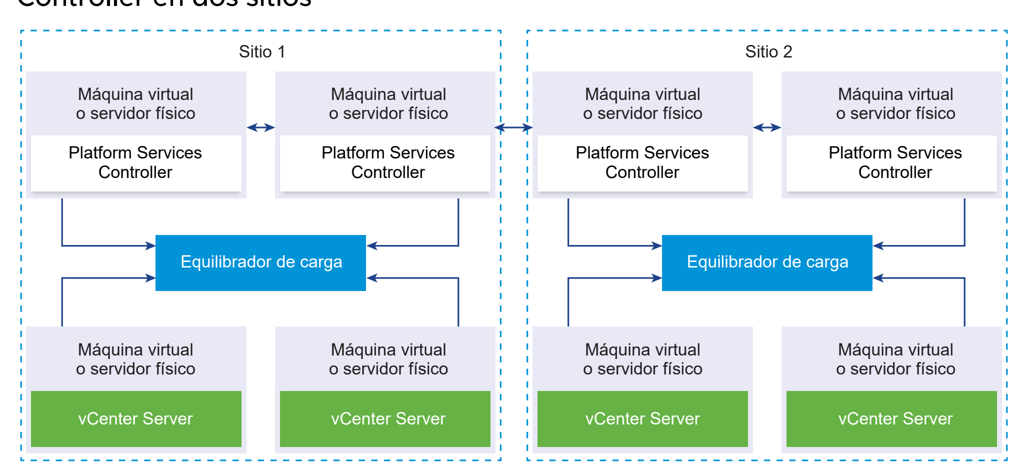
Es posible utilizar un equilibrador de carga de terceros por sitio para configurar la alta disponibilidad de Platform Services Controller con conmutación por error automática para ese sitio. Para obtener información sobre la cantidad máxima de instancias de Platform Services Controller detrás de un equilibrador de carga, consulte la documentación de *Máximos de configuración*.

Importante Para configurar la alta disponibilidad de Platform Services Controller detrás de un equilibrador de carga, las instancias de Platform Services Controller deben estar en el mismo tipo de sistema operativo. No se admiten las instancias de Platform Services Controller detrás de un equilibrador de carga en sistemas operativos combinados.

Las instancias de vCenter Server se conectan al equilibrador de carga. Cuando una instancia de Platform Services Controller deja de responder, el equilibrador de carga distribuye automáticamente la carga entre las otras instancias de Platform Services Controller en funcionamiento sin producir tiempo de inactividad.

Platform Services Controller con equilibradores de carga en sitios de vCenter Single Sign-On

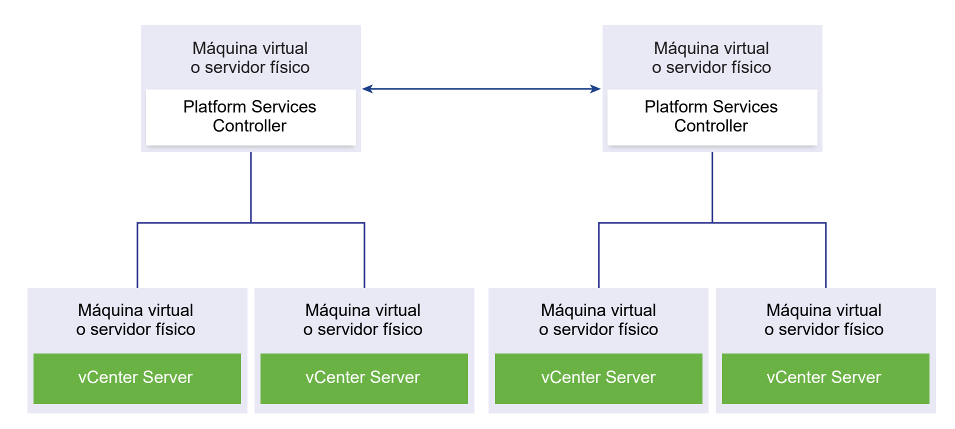
Figura 1-6. Ejemplo de dos pares con carga equilibrada de instancias de Platform Services Controller en dos sitios



El dominio de vCenter Single Sign-On puede abarcar varios sitios. Para garantizar la alta disponibilidad de Platform Services Controller con conmutación por error automática en todo el dominio, es necesario configurar un equilibrador de carga separado en cada sitio.

Platform Services Controller sin equilibrador de carga

Figura 1-7. Ejemplo de dos instancias unidas de Platform Services Controller sin ningún equilibrador de carga



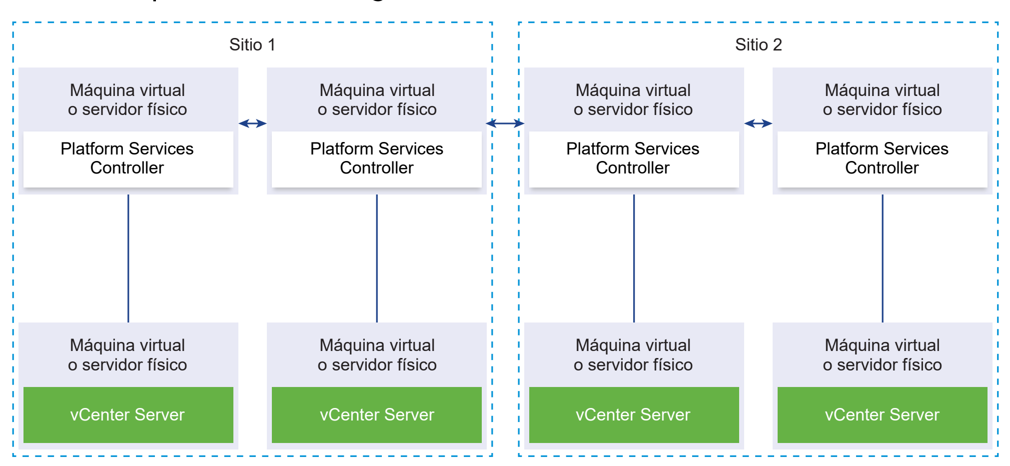
Cuando se unen dos o más instancias de Platform Services Controller en un mismo sitio sin ningún equilibrador de carga, se debe configurar la alta disponibilidad de Platform Services Controller con una conmutación por error manual para ese sitio.

Cuando una instancia de Platform Services Controller deja de responder, se deben conmutar manualmente las instancias de vCenter Server que están registradas en ella. Para conmutar las instancias, es necesario redirigirlas a otras instancias funcionales de Platform Services Controller dentro del mismo sitio. Para obtener información sobre la forma de redirigir instancias de vCenter Server a otra instancia externa de Platform Services Controller, consulte *Instalar y configurar vCenter Server*.

Nota Si su dominio de vCenter Single Sign-On incluye tres o más instancias de Platform Services Controller, puede crear manualmente una topología de anillo. Una topología de anillo garantiza la confiabilidad de Platform Services Controller cuando se produce un error en una de las instancias. Para crear una topología de anillo, ejecute el comando `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` en la primera y la última instancia de Platform Services Controller que implementó.

Platform Services Controller sin ningún equilibrador de carga en sitios de vCenter Single Sign-On

Figura 1-8. Ejemplo de dos pares unidos de instancias de Platform Services Controller en dos sitios sin equilibrador de carga



El dominio de vCenter Single Sign-On puede abarcar varios sitios. Cuando no existe ningún equilibrador de carga disponible, es posible redirigir manualmente vCenter Server de una instancia con errores a una instancia en funcionamiento de Platform Services Controller dentro del mismo sitio. Para obtener información sobre la forma de redirigir instancias de vCenter Server a otra instancia externa de Platform Services Controller, consulte *Instalar y configurar vCenter Server*.

Comprender los sitios, los nombres de dominio y los dominios de vSphere

Cada instancia de Platform Services Controller está asociada con un dominio de vCenter Single Sign-On. El valor predeterminado del nombre de dominio es vsphere.local, pero puede cambiarlo durante la instalación de la primera instancia de Platform Services Controller. El dominio determina el espacio de autenticación local. Puede dividir un dominio en varios sitios, y asignar cada instancia de Platform Services Controller y vCenter Server a un sitio. Los sitios son construcciones lógicas, pero generalmente corresponden a la ubicación geográfica.

Dominio de Platform Services Controller

Cuando instale una instancia de Platform Services Controller, se le solicitará que cree un dominio de vCenter Single Sign-On o que se una a un dominio existente.

VMware Directory Service (vmdir) usa el nombre del dominio para todas las estructuras internas del Protocolo Simplificado de Acceso a Directorios (LDAP).

Con vSphere 6.0 y posterior, puede dar a su dominio de vSphere un nombre único. Para evitar conflictos de autenticación, use un nombre que OpenLDAP, Microsoft Active Directory y otros servicios de directorio no usen.

Nota No puede cambiar el dominio al que pertenece una instancia de Platform Services Controller o vCenter Server.

Después de especificar el nombre para el dominio, puede agregar usuarios y grupos. Normalmente es mejor agregar un origen de identidad de Active Directory o LDAP, y permitir a los usuarios y grupos de dicho origen que autentiquen. También puede agregar al dominio instancias de vCenter Server o Platform Services Controller, o bien otros productos VMware como vRealize Operations.

Sitios de Platform Services Controller

Puede organizar los dominios de Platform Services Controller en sitios lógicos. Un sitio de VMware Directory Service es un contenedor lógico para agrupar instancias de Platform Services Controller dentro de un dominio de vCenter Single Sign-On.

Desde vSphere 6.5, los sitios son importantes. Durante la conmutación por error de Platform Services Controller, las instancias de vCenter Server se vuelven afines a una instancia de Platform Services Controller diferente en el mismo sitio. Para impedir que sus instancias de vCenter Server se vuelvan afines a una instancia de Platform Services Controller en una ubicación geográfica distante, puede usar varios sitios.

Se le pedirá el nombre de sitio al instalar o actualizar una instancia de Platform Services Controller. Consulte la documentación de *Instalar y configurar vCenter Server*.

Capacidades de Platform Services Controller

Platform Services Controller admite servicios como la administración de identidades, de certificados y de licencias en vSphere.

Capacidades clave

Platform Services Controller incluye varios servicios, los cuales se explican en Servicios de Platform Services Controller, y cuenta con las siguientes capacidades clave.

- Autenticación a través de vCenter Single Sign-On
- Aprovisionamiento predeterminado de los componentes de vCenter Server y los hosts ESXi con certificados de VMware Certificate Manager (VMCA)
- Uso de certificados personalizados, que se almacenan en VMware Endpoint Certificate Store (VECS)

Modelos de implementación

Puede instalar Platform Services Controller en un sistema con Windows o implementar el dispositivo de Platform Services Controller.

El modelo de implementación depende de la versión de Platform Services Controller que esté utilizando. Consulte Tipos de implementación de vCenter Server y Platform Services Controller.

A partir de vSphere 6.7 Update 1, si implementó o instaló una instancia de vCenter Server con una instancia externa de Platform Services Controller y quiere convertirla a vCenter Server con una instancia integrada de Platform Services Controller, puede replicar una nueva instancia de Platform Services Controller que está integrada en la instancia existente de vCenter Server. Consulte la documentación de *Instalar y configurar vCenter Server*.

A partir de vSphere 6.7 Update 1, puede mover una instancia de vCenter Server con una instancia integrada de Platform Services Controller desde un dominio de vSphere hasta otro dominio de vSphere. Los servicios como el etiquetado y la concesión de licencias se conservan y se migran a un nuevo dominio. Consulte la documentación de *Instalar y configurar vCenter Server*.

Administrar servicios de Platform Services Controller

Los servicios de Platform Services Controller se pueden administrar desde vSphere Client con uno de los scripts o las CLI disponibles.

Los diferentes servicios de Platform Services Controller admiten diferentes interfaces.

Tabla 1-2. Interfaces para administrar servicios de Platform Services Controller

Interfaz	Descripción
vSphere Client	Interfaz web (cliente basado en HTML5). La terminología, la topología y el flujo de trabajo de la interfaz de usuario de vSphere Client están estrechamente relacionados con los mismos aspectos y elementos de la interfaz de usuario de vSphere Web Client.
vSphere Web Client	Interfaz web para administrar algunos de los servicios.
Utilidad de administración de certificados	Herramienta de línea de comandos que permite generar CSR y reemplazar certificados. Consulte Administrar certificados con la utilidad vSphere Certificate Manager.
CLI para administrar servicios de Platform Services Controller	Conjunto de comandos para administrar certificados, el almacén de certificados de endpoints de VMware (VECS) y VMware Directory Service (vmdir). Consulte Capítulo 4 Administrar servicios y certificados con comandos de CLI.

Servicios de Platform Services Controller

Con Platform Services Controller, todos los productos VMware del mismo entorno pueden compartir el dominio de autenticación y otros servicios. Los servicios incluyen la administración de certificados, la autenticación y las licencias.

Platform Services Controller incluye los siguientes servicios de infraestructura básicos.

Tabla 1-3. Servicios de Platform Services Controller

Servicio	Descripción
`applmgmt` (VMware Appliance Management Service)	Gestiona la configuración del dispositivo y proporciona endpoints de API pública para la administración del ciclo de vida del dispositivo. Se incluye en el dispositivo de Platform Services Controller.
`vmware-cis-license` (VMware License Service)	Cada instancia de Platform Services Controller incluye VMware License Service, que proporciona funcionalidad centralizada de administración e informes de licencias para los productos VMware de su entorno. El inventario del servicio de licencias se replica en todas las instancias de Platform Services Controller del dominio cada 30 segundos.
`vmware-stsd` (VMware Security Token Service)	Servicio tras la función vCenter Single Sign-On, que proporciona servicios de autenticación segura para los usuarios y los componentes de software de VMware. Al usar vCenter Single Sign-On, los componentes de VMware se comunican utilizando un mecanismo de intercambio de tokens SAML seguro. vCenter Single Sign-On construye un dominio de seguridad interno (vsphere.local de forma predeterminada) en el que los componentes de software de VMware se registran durante la instalación o la actualización.
`vmware-rhttpproxy` (VMware HTTP Reverse Proxy)	El proxy inverso se ejecuta en todos los nodos de Platform Services Controller y todos los sistemas de vCenter Server. Se trata de un punto de entrada único al nodo que permite que los servicios que se ejecutan en él se comuniquen de forma segura.
`vmware-sca` (VMware Service Control Agent)	Administra las configuraciones de los servicios. Puede utilizar la CLI de `service-control` para administrar configuraciones individuales de los servicios.
`vmware-statsmonitor` (Servicio de supervisión de VMware Appliance)	Supervisa el consumo de recursos del sistema operativo invitado de vCenter Server Appliance.
`vmware-vapi-endpoint` (VMware vAPI Endpoint)	vSphere Automation API Endpoint proporciona un punto de acceso único a los servicios de vAPI. Puede cambiar las propiedades del servicio de vAPI Endpoint desde vSphere Client. Consulte la *guía de programación de vSphere Automation SDK* para obtener información sobre las instancias de vAPI Endpoint.
`vmafdd` VMware Authentication Framework	Servicio que proporciona un marco del lado cliente para la autenticación de vmdir y sirve a VMware Endpoint Certificate Store (VECS).

Tabla 1-3. Servicios de Platform Services Controller (continuación)

Servicio	Descripción
`vmcad` VMware Certificate Service	Aprovisiona a todos los componentes de software de VMware que tengan las bibliotecas de cliente de vmafd y a todos los hosts ESXi con un certificado firmado que tengan a VMCA como entidad de certificación raíz. Puede cambiar los certificados predeterminados a través de la utilidad Certificate Manager. VMware Certificate Service utiliza VMware Endpoint Certificate Store (VECS) para que sirva como repositorio local para los certificados en todas las instancias de Platform Services Controller. Aunque puede abstenerse de utilizar VMCA y, en su lugar, utilizar certificados personalizados, deberá agregar los certificados a VECS.
`vmdird` VMware Directory Service	Proporciona un servicio de directorios LDAP de varios tenants y replicación de pares que almacena información sobre autenticación, certificados, búsquedas y licencias. No actualice datos en `vmdird` a través de un explorador de LDAP. Si su dominio contiene más de una instancia de Platform Services Controller, una actualización del contenido de una instancia de vmdir se propaga a todas las demás.
`vmdnsd` VMware Domain Name Service	No se utiliza en vSphere 6.x.
`vmonapi` API de VMware Lifecycle Manager `vmware-vmon` VMware Service Lifecycle Manager	Inicia y detiene los servicios de vCenter Server y supervisa el estado de la API del servicio. `vmware-vmon` es un servicio centralizado y no dependiente de ninguna plataforma que administra el ciclo de vida de Platform Services Controller y vCenter Server. Expone las API y las CLI a aplicaciones de terceros.
`lwsmd` Likewise Service Manager	Likewise facilita la unión del host a un dominio de Active Directory y la posterior autenticación del usuario.
`pschealth` Monitor de estado de VMware Platform Services Controller	Supervisa el estado de todos los servicios centrales de la infraestructura de Platform Services Controller.
`vmware-analytics` Servicio de análisis de VMware	Consta de componentes que recopilan datos de telemetría de diversos componentes de vSphere y los cargan a la nube de análisis de VMware, y administran el Programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP).

Administrar servicios de Platform Services Controller desde vSphere Client

Puede administrar el inicio de sesión único, los certificados, los dominios vinculados, las soluciones, las licencias y el control de acceso de vCenter desde vSphere Client.

Procedimiento

1 Inicie sesión en un servidor vCenter Server asociado con Platform Services Controller como usuario con privilegios de administrador en el dominio de vCenter Single Sign-On local (vsphere.local de manera predeterminada).

2 Seleccione **Administración** y haga clic en el elemento que quiera administrar.

Administrar servicios de Platform Services Controller desde vSphere Web Client

Puede administrar vCenter Single Sign-On y el servicio de licencias desde vSphere Web Client.

Use vSphere Client o las CLI en lugar de vSphere Web Client para administrar los siguientes servicios.

- Certificados
- Almacén de certificados de endpoints de VMware (VECS)
- Autenticación de dos factores como la autenticación de tarjeta de acceso común
- Aviso de inicio de sesión

Procedimiento

1 Inicie sesión en un servidor vCenter Server asociado con Platform Services Controller como usuario con privilegios de administrador en el dominio de vCenter Single Sign-On local (vsphere.local de manera predeterminada).

2 Seleccione **Administración** y haga clic en el elemento que quiera administrar.

Opción	Descripción
Single Sign-On	Configure vCenter Single Sign-On. ■ Establezca las directivas. ■ Administre los orígenes de identidad. ■ Administre el certificado de firma de STS. ■ Administre los proveedores de servicios SAML. ■ Administre usuarios y grupos.
Licencias	Configure las licencias.

Usar scripts para administrar servicios de Platform Services Controller

Platform Services Controller incluye scripts para generar solicitudes de firma del certificado (Certificate Signing Request, CSR), administrar certificados y administrar servicios.

Por ejemplo, puede usar la utilidad `certool` a fin de generar CSR y reemplazar certificados para escenarios con instancias integradas de Platform Services Controller y para escenarios con instancias externas de Platform Services Controller. Consulte Administrar certificados con la utilidad vSphere Certificate Manager.

Use las CLI para tareas de administración que las interfaces web no admitan o para crear scripts personalizados para el entorno.

Tabla 1-4. CLI para administrar certificados y servicios relacionados

CLI	Descripción	Vínculos
`certool`	Genere y administre certificados y claves. Parte de VMCA.	Referencia de comandos de inicialización de certool
`vecs-cli`	Administre el contenido de las instancias de VMware Certificate Store. Parte de VMAFD.	Referencia de comandos vecs-cli
`dir-cli`	Cree y actualice los certificados en VMware Directory Service. Parte de VMAFD.	Referencia de comando dir-cli
`sso-config`	Utilidad para configurar la autenticación de tarjetas inteligentes.	Descripción de la autenticación de dos factores de vCenter Server
`service-control`	Comando para iniciar, detener y armar una lista de servicios.	Ejecute este comando para detener servicios antes de ejecutar otros comandos de CLI.

Procedimiento

1 Inicie sesión en el shell de Platform Services Controller.

En la mayoría de los casos, debe ser el usuario raíz o administrador. Consulte Privilegios necesarios para ejecutar CLI para obtener detalles.

2 Acceda a la CLI en una de las siguientes ubicaciones predeterminadas.

Los privilegios necesarios dependen de la tarea que se desea realizar. En algunos casos, se solicita que introduzca la contraseña dos veces para proteger información confidencial.

Windows

`C:\Archivos de programa\VMware\vCenter Server\vmafdd\vecs-cli.exe`

`C:\Archivos de programa\VMware\vCenter Server\vmafdd\dir-cli.exe`

`C:\Archivos de programa\VMware\vCenter Server\vmcad\certool.exe`

`C:\Archivos de programa\VMware\VCenter server\VMware Identity Services\sso-config`

RUTA_DE_INSTALACIÓN_DE_VCENTER`\bin\service-control`

Linux

`/usr/lib/vmware-vmafd/bin/vecs-cli`

`/usr/lib/vmware-vmafd/bin/dir-cli`

`/usr/lib/vmware-vmca/bin/certool`

`/opt/vmware/bin`

En Linux, el comando `service-control` no requiere que especifique la ruta de acceso.

Administración del dispositivo de Platform Services Controller

Puede administrar el dispositivo de Platform Services Controller desde la interfaz de administración de dispositivos virtuales o el shell del dispositivo.

Si utiliza un entorno con Platform Services Controller integrado, administra un dispositivo que incluye Platform Services Controller y vCenter Server. Consulte *Configuración de vCenter Server Appliance*.

Tabla 1-5. Interfaces para administrar el dispositivo de Platform Services Controller

Interfaz	Descripción
Interfaz de administración de dispositivos virtuales (VAMI) de Platform Services Controller	Use esta interfaz para volver a configurar los parámetros del sistema de una implementación de Platform Services Controller.
Shell del dispositivo de Platform Services Controller	Use esta interfaz de línea de comandos para realizar operaciones de administración de servicios en VMCA, VECS y VMDIR. Consulte Administrar certificados con la utilidad vSphere Certificate Manager y Capítulo 4 Administrar servicios y certificados con comandos de CLI.

Administrar el dispositivo con la interfaz de administración de dispositivos virtuales de Platform Services Controller

En los entornos con una instancia externa de Platform Services Controller, es posible usar la interfaz de administración de dispositivos virtuales (Virtual Appliance Management Interface, VAMI) de Platform Services Controller para definir la configuración del sistema del dispositivo. La configuración incluye la sincronización de hora, la configuración de red y los ajustes de inicio de sesión en SSH. También es posible cambiar la contraseña raíz, unir el dispositivo a un dominio de Active Directory y abandonar un dominio de Active Directory.

En los entornos con un Platform Services Controller integrado, es posible administrar los dispositivos que incluyen Platform Services Controller y vCenter Server.

Procedimiento

1 En un explorador web, vaya a la interfaz web en https://*platform_services_controller_ip*:5480.

2 Si aparece un mensaje de advertencia sobre un certificado SSL que no es de confianza, solucione el problema en función de la directiva de seguridad de la empresa y el explorador web que está usando.

3 Inicie sesión como raíz.

La contraseña raíz predeterminada es la contraseña raíz del dispositivo virtual que configuró al implementar el dispositivo virtual.

Resultados

Puede consultar la página Información del sistema de la interfaz de administración de dispositivos de Platform Services Controller.

Administrar el dispositivo desde su propio shell

Puede emplear utilidades de administración de servicios y CLI del shell del dispositivo. Puede usar TTY1 para iniciar sesión en la consola, o bien SSH para conectarse al shell.

Procedimiento

1 Habilite el inicio de sesión en SSH si resulta necesario.

   a Inicie sesión en la interfaz de administración de dispositivos (Appliance Management Interface, VAMI) en https://*platform_services_controller_ip*:5480.

   b En el navegador, seleccione **Acceso** y haga clic en **Editar**.

   c Active **Habilitar el inicio de sesión SSH** y haga clic en **Aceptar**.

   Puede seguir los mismos pasos para habilitar el shell de Bash para el dispositivo.

2 Acceda al shell del dispositivo.

   - Si tiene acceso directo a la consola del dispositivo, seleccione **Iniciar sesión** y presione Intro.
   - Para conectarse de forma remota, utilice SSH u otra conexión de consola remota para iniciar una sesión en el dispositivo.

3 Inicie sesión como raíz con la contraseña que configuró mientras implementaba inicialmente el dispositivo.

   Si cambió la contraseña raíz, use la nueva contraseña.

Agregar un dispositivo de Platform Services Controller a un dominio de Active Directory

Si desea agregar un origen de identidad de Active Directory a Platform Services Controller, primero debe unir el dispositivo de Platform Services Controller a un dominio de Active Directory.

Si está usando una instancia de Platform Services Controller que está instalada en Windows, puede usar el dominio al que pertenece esa máquina.

Procedimiento

1 Mediante vSphere Client, inicie sesión en una instancia de vCenter Server asociada con Platform Services Controller como un usuario con privilegios de administrador en el dominio local de vCenter Single Sign-On (vsphere.local de forma predeterminada).

2 Seleccione **Administración**.

3 Expanda **Single Sign-On** y haga clic en **Configuración**.

4 Haga clic en **Dominio de Active Directory**.

5 Haga clic en **Unirse a dominio de AD**, especifique el dominio, la unidad organizativa opcional, un nombre de usuario y una contraseña; a continuación, haga clic en **Unirse**.

Pasos siguientes

Para asociar usuarios y grupos del dominio de Active Directory al que se unió, agregue dicho dominio como un origen de identidad de vCenter Single Sign-On. Consulte Agregar o editar un origen de identidad vCenter Single Sign-On.

Autenticar vSphere con vCenter Single Sign-On

2

vCenter Single Sign-On es un agente de autenticación y una infraestructura de intercambio de tokens de seguridad. Cuando un usuario puede autenticarse en vCenter Single Sign-On, recibe el token SAML. Posteriormente, el usuario puede utilizar el token SAML para autenticarse en los servicios de vCenter. Luego, el usuario puede realizar las acciones para las que tiene privilegios.

Ya que el tráfico está cifrado para todas las comunicaciones y solo los usuarios autenticados puede realizar las acciones para las que tienen privilegios, el entorno permanece seguro.

A partir de vSphere 6.0, vCenter Single Sign-On forma parte de Platform Services Controller. Platform Services Controller contiene servicios compartidos que admiten componentes de vCenter Server y vCenter Server. Estos servicios incluyen vCenter Single Sign-On, VMware Certificate Authority y el servicio de licencias. Consulte *Instalar y configurar vCenter Server* para obtener detalles sobre Platform Services Controller.

En el protocolo de enlace inicial, los usuarios se autentican con un nombre de usuario y una contraseña, mientras que los usuarios de solución lo hacen con un certificado. Para obtener información sobre el reemplazo de certificados de usuario de solución, consulte Capítulo 3 Certificados de seguridad de vSphere.

El siguiente paso es autorizar a los usuarios que pueden autenticar a que realicen ciertas tareas. En la mayoría de los casos, usted asigna privilegios de vCenter Server, generalmente asignando el usuario a un grupo con una función. vSphere incluye otros modelos de permiso como permisos globales. Consulte la documentación de *Seguridad de vSphere*.

Este capítulo incluye los siguientes temas:

- Descripción general de vCenter Single Sign-On
- Configurar orígenes de identidad de vCenter Single Sign-On
- Descripción de la autenticación de dos factores de vCenter Server
- Utilizar vCenter Single Sign-On como el proveedor de identidad para otro proveedor de servicios
- Servicio de token de seguridad (STS)
- Administrar directivas de vCenter Single Sign-On
- Administrar usuarios y grupos de vCenter Single Sign-On
- Prácticas recomendadas de seguridad de vCenter Single Sign-On

Descripción general de vCenter Single Sign-On

Para administrar vCenter Single Sign-On de forma efectiva, debe comprender la arquitectura subyacente y cómo esta afecta la instalación y las actualizaciones.



Dominios y sitios de vCenter Single Sign-On 6.0 (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_y9pxac75/uiConfId/49694343/)

Cómo vCenter Single Sign-On protege el entorno

vCenter Single Sign-On permite que los componentes de vSphere se comuniquen entre sí a través de un mecanismo de token seguro.

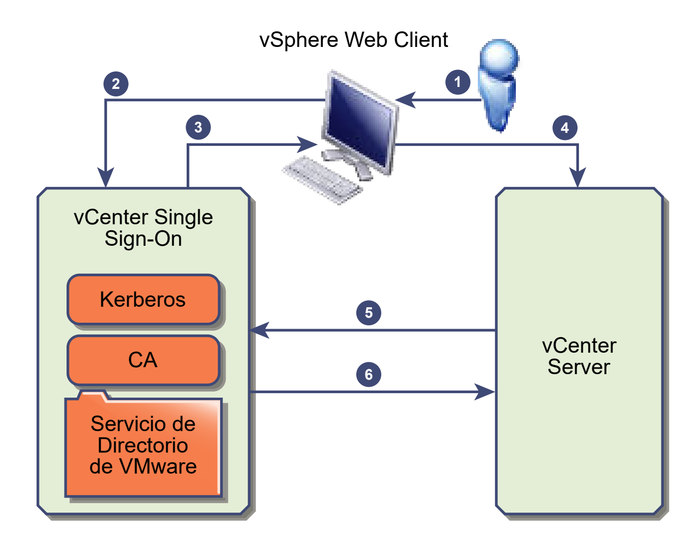
vCenter Single Sign-On utiliza los siguientes servicios.

- STS (servicio de token de seguridad).
- SSL para proteger el tráfico.
- La autenticación de usuarios humanos a través de Active Directory u OpenLDAP.
- La autenticación de usuarios de soluciones a través de certificados.

Protocolo de enlace de vCenter Single Sign-On para usuarios humanos

En la siguiente ilustración se muestra el protocolo de enlace para usuarios humanos.

Figura 2-1. Protocolo de enlace de vCenter Single Sign-On para usuarios humanos



1 El usuario inicia sesión en vSphere Client con un nombre de usuario y una contraseña para acceder al sistema vCenter Server o a otro servicio de vCenter.

  El usuario también puede iniciar sesión sin una contraseña y activar la casilla **Usar la autenticación de sesión de Windows**.

2 vSphere Client pasa la información de inicio de sesión al servicio vCenter Single Sign-On, que comprueba el token SAML de vSphere Client. Si vSphere Client tiene un token válido, vCenter Single Sign-On comprueba si el usuario se encuentra en el origen de identidad configurado (por ejemplo, Active Directory).

   - Si solo se emplea el nombre de usuario, vCenter Single Sign-On comprueba el dominio predeterminado.
   - Si se incluye un nombre de dominio con el nombre de usuario (*DOMAIN*\user1 o user1@*DOMAIN*), vCenter Single Sign-On comprueba ese dominio.

3 Si el usuario puede autenticarse en el origen de identidad, vCenter Single Sign-On devuelve un token que representa al usuario en vSphere Client.

4 vSphere Client pasa el token al sistema vCenter Server.

5 vCenter Server comprueba con el servidor de vCenter Single Sign-On que el token sea válido y que no haya caducado.

6 El servidor de vCenter Single Sign-On devuelve el token al sistema vCenter Server mediante el marco de autorización de vCenter Server para otorgar acceso a los usuarios.

Ahora el usuario puede autenticarse, y ver y modificar todos los objetos sobre los que tiene privilegios por su función.

Nota Al principio, se asigna la función Sin acceso a cada usuario. Un administrador de vCenter Server debe asignar al menos la función Solo lectura al usuario para que pueda iniciar sesión. Consulte la documentación de *Seguridad de vSphere*.

Protocolo de enlace de vCenter Single Sign-On para usuarios de solución

Los usuarios de solución son conjuntos de servicios que se usan en la infraestructura de vCenter Server, por ejemplo, vCenter Server o las extensiones de vCenter Server. Las extensiones de VMware y las posibles extensiones externas también pueden autenticarse en vCenter Single Sign-On.

Figura 2-2. Protocolo de enlace de vCenter Single Sign-On para usuarios de solución

En el caso de los usuarios de solución, la interacción se produce de la siguiente manera:

1 El usuario de la solución intenta conectarse a un servicio de vCenter.

2 Se redirige al usuario de solución a vCenter Single Sign-On. Si el usuario de solución es nuevo en vCenter Single Sign-On, debe presentar un certificado válido.

3 Si el certificado es válido, vCenter Single Sign-On asigna un token SAML (token de portador) al usuario de solución. vCenter Single Sign-On firma el token.

4 El usuario de solución se redirige a vCenter Single Sign-On y puede realizar tareas según sus permisos.

5 La próxima vez que el usuario de solución deba autenticarse, podrá usar el token SAML para iniciar sesión en vCenter Server.

De forma predeterminada, este protocolo de enlace se aplica automáticamente, ya que VMCA aprovisiona a los usuarios de solución con certificados durante el inicio. Si la directiva de la empresa exige certificados externos firmados por una entidad de certificación, se pueden utilizar esos certificados para reemplazar los certificados de los usuarios de solución. Si esos certificados son válidos, vCenter Single Sign-On asigna un token SAML al usuario de solución. Consulte Usar certificados personalizados con vSphere.

Cifrado compatible

Se admite el cifrado AES, que es el nivel más alto de cifrado. El cifrado compatible también afecta a la seguridad cuando vCenter Single Sign-On utiliza Active Directory como un origen de identidad.

También afecta a la seguridad cada vez que un host ESXi o vCenter Server se une a Active Directory.

Componentes de vCenter Single Sign-On

vCenter Single Sign-On incluye el servicio de token de seguridad (STS), un servidor de administración y vCenter Lookup Service, además de VMware Directory Service (vmdir). VMware Directory Service también se usa para la administración de certificados.

Durante la instalación, los componentes se implementan como parte de una implementación integrada o como parte de Platform Services Controller.

STS (servicio de token de seguridad)

El servicio STS emite tokens de lenguaje de marcado de aserción de seguridad (Security Assertion Markup Language, SAML). Estos tokens de seguridad representan la identidad de un usuario en uno de los tipos de orígenes de identidad compatibles con vCenter Single Sign-On. Los tokens de SAML permiten que los usuarios humanos y los usuarios de soluciones que se autentican correctamente en vCenter Single Sign-On utilicen cualquier servicio de vCenter que sea compatible con vCenter Single Sign-On sin tener que volver a autenticarse en cada servicio.

El servicio vCenter Single Sign-On firma todos los tokens con un certificado de firma y almacena el certificado de firma de tokens en el disco. El certificado del propio servicio también se almacena en el disco.

Servidor de administración

El servidor de administración permite que los usuarios con privilegios de administrador para vCenter Single Sign-On configuren el servidor vCenter Single Sign-On y administren usuarios y grupos de vSphere Web Client. Inicialmente, solo el usuario administrator@*your_domain_name* tenía estos privilegios. En vSphere 5.5, este usuario era administrator@vsphere.local. Con vSphere 6.0, puede cambiar el dominio de vSphere cuando instale vCenter Server o implemente vCenter Server Appliance con una nueva instancia de Platform Services Controller. No asigne el nombre de dominio de Microsoft Active Directory u OpenLDAP a su nombre de dominio.

VMware Directory Service (vmdir)

VMware Directory Service (vmdir) se asocia al dominio que especifique durante la instalación y se incluye en todas las implementaciones integradas y en cada Platform Services Controller. Se trata de un servicio de directorio multiempresa y con varios maestros que pone a disposición un directorio LDAP en el puerto 389. El servicio aún utiliza el puerto 11711 para la compatibilidad con versiones anteriores de vSphere 5.5 y sistemas anteriores.

Si su entorno incluye más de una instancia de Platform Services Controller, se propaga una actualización del contenido de vmdir de una instancia de vmdir a todas las demás.

A partir de vSphere 6.0, VMware Directory Service no solo almacena información de vCenter Single Sign-On, sino también información sobre certificados.

Servicio de administración de identidades

Controla los orígenes de identidad y las solicitudes de autenticación de STS.

Cómo influye vCenter Single Sign-On en la instalación

A partir de la versión 5.1, vSphere incluye un servicio vCenter Single Sign-On como parte de la infraestructura de administración de vCenter Server. Este cambio afecta la instalación de vCenter Server.

La autenticación con vCenter Single Sign-On refuerza la seguridad de vSphere porque los componentes de software de vSphere se comunican entre sí a través de un mecanismo de intercambio de token seguro. Además, todos los otros usuarios también se autentican con vCenter Single Sign-On.

A partir de vSphere 6.0, vCenter Single Sign-On se incluye en una implementación integrada o como parte de Platform Services Controller. Platform Services Controller contiene todos los servicios necesarios para la comunicación entre los componentes de vSphere, incluidos vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service y el servicio de licencias.

El orden de instalación es importante.

Primera instalación

Si se trata de una instalación distribuida, debe instalar Platform Services Controller antes de instalar vCenter Server o implementar vCenter Server Appliance. Para una implementación integrada, el orden de instalación correcto se produce en forma automática.

Instalaciones subsiguientes

Para hasta cuatro instancias de vCenter Server aproximadamente, una instancia de Platform Services Controller puede servir todo el entorno de vSphere. Puede conectar las nuevas instancias de vCenter Server a la misma instancia de Platform Services Controller. Para más de cuatro instancias de vCenter Server aproximadamente, puede instalar una instancia de Platform Services Controller adicional para obtener un mejor rendimiento. El servicio vCenter Single Sign-On de cada Platform Services Controller sincroniza los datos de autenticación con todas las demás instancias. El número exacto depende de cuánto se utilicen las instancias de vCenter Server y de otros factores.

Para obtener información detallada sobre los modelos de implementación, así como de las ventajas y las desventajas de cada tipo de implementación, consulte *Instalar y configurar vCenter Server*.

Usar vCenter Single Sign-On con vSphere

Cuando un usuario inicia sesión en un componente de vSphere o cuando un usuario de solución de vCenter Server accede a otro servicio de vCenter Server, vCenter Single Sign-On lleva a cabo la autenticación. Los usuarios deben autenticarse con vCenter Single Sign-On y tener los privilegios necesarios para interactuar con objetos de vSphere.

vCenter Single Sign-On autentica a los usuarios de solución y a otros usuarios.

- Los usuarios de solución representan un conjunto de servicios en el entorno de vSphere. Durante la instalación, VMCA asigna un certificado a cada usuario de solución de forma predeterminada. El usuario de solución utiliza ese certificado para autenticarse en vCenter Single Sign-On. vCenter Single Sign-On otorga al usuario de solución un token SAML para que pueda interactuar con otros servicios del entorno.
- Cuando otros usuarios inician sesión en el entorno, por ejemplo, desde vSphere Client, vCenter Single Sign-On solicita un nombre de usuario y una contraseña. Si vCenter Single Sign-On encuentra un usuario con esas credenciales en el origen de identidad correspondiente, le asigna un token SAML. De esta forma, el usuario puede acceder a otros servicios del entorno sin tener que autenticarse de nuevo.

  Los objetos que el usuario puede ver y lo que este puede hacer están determinados por los parámetros de configuración de permiso de vCenter Server. Los administradores de vCenter Server asignan esos permisos desde la interfaz **Permisos** en vSphere Web Client o vSphere Client, no a través de vCenter Single Sign-On. Consulte la documentación de *Seguridad de vSphere*.

Usuarios de vCenter Single Sign-On y vCenter Server

Los usuarios se autentican en vCenter Single Sign-On introduciendo sus credenciales en la página de inicio de sesión. Después de conectarse a vCenter Server, los usuarios autenticados pueden ver todas las instancias de vCenter Server u otros objetos de vSphere para los que su función les da privilegios. En esta instancia ya no se requiere autenticación adicional.

Después de la instalación, el administrador del dominio de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada, tiene acceso de administrador tanto a vCenter Single Sign-On como a vCenter Server. Ese usuario puede agregar orígenes de identidad, establecer el origen de identidad predeterminado y administrar usuarios y grupos en el dominio de vCenter Single Sign-On.

Todos los usuarios que pueden autenticarse en vCenter Single Sign-On pueden restablecer su contraseña, incluso si esta ha caducado, siempre y cuando la sepan. Consulte Cambiar la contraseña de vCenter Single Sign-On. Solo los administradores de vCenter Single Sign-On pueden restablecer la contraseña de los usuarios que ya no tienen su contraseña.

Nota Al cambiar la contraseña del SDDC desde vSphere Client, la nueva contraseña no se sincroniza con aquella que se muestra en la página Credenciales predeterminadas de vCenter. En esa página, solo se muestran las credenciales predeterminadas. Si cambia las credenciales, debe realizar un seguimiento de la nueva contraseña. Póngase en contacto con el equipo de soporte técnico y solicite un cambio de contraseña.

Usuarios administradores de vCenter Single Sign-On

Desde vSphere Client o vSphere Web Client, puede accederse a la interfaz de administración de vCenter Single Sign-On.

Para configurar vCenter Single Sign-On y administrar usuarios y grupos de vCenter Single Sign-On, el usuario administrator@vsphere.local o un usuario del grupo de administradores de vCenter Single Sign-On deben iniciar sesión en vSphere Client. Después de la autenticación, el usuario puede acceder a la interfaz de administración de vCenter Single Sign-On desde vSphere Client y administrar orígenes de identidad y dominios predeterminados, especificar directivas de contraseñas y realizar otras tareas administrativas.

Nota No puede cambiar el nombre de usuario administrador de vCenter Single Sign-On, que es administrator@vsphere.local de manera predeterminada o administrator@*mydomain* si especificó un dominio diferente durante la instalación. Para mejorar la seguridad, se recomienda que cree usuarios designados adicionales en el dominio vCenter Single Sign-On y les asigne privilegios administrativos. Luego puede dejar de usar la cuenta de administrador.

Usuarios de ESXi

Los hosts ESXi independientes no están integrados con vCenter Single Sign-On ni con Platform Services Controller. Consulte *Seguridad de vSphere* para obtener información sobre cómo agregar un host ESXi a Active Directory.

Si crea usuarios ESXi locales para un host ESXi administrado con VMware Host Client, vCLI o PowerCLI, vCenter Server no sabe quiénes son esos usuarios. Por ello, la creación de usuarios locales puede derivar en confusión, especialmente si usa los mismos nombres de usuario. Los usuarios que pueden autenticar en vCenter Single Sign-On pueden ver y administrar hosts ESXi si tienen los permisos correspondiente en el objeto de host ESXi.

Nota De ser posible, administre los permisos de hosts ESXi mediante vCenter Server.

Cómo iniciar sesión en componentes de vCenter Server

Puede iniciar sesión conectándose a vSphere Client o vSphere Web Client.

Cuando un usuario inicia sesión en un sistema vCenter Server desde vSphere Client, el comportamiento de inicio de sesión depende de si el usuario se encuentra o no en el dominio configurado como el origen de identidad predeterminado.

- Los usuarios que están en el dominio predeterminado pueden iniciar sesión con su nombre de usuario y contraseña.
- Los usuarios que están en un dominio que se ha agregado a vCenter Single Sign-On como un origen de identidad, pero que no es el dominio predeterminado, pueden iniciar sesión en vCenter Server, pero deben especificar el dominio de una de las siguientes maneras.
  - Incluyendo un prefijo de nombre de dominio; por ejemplo, MIDOMINIO\usuario1.
  - Incluyendo el dominio; por ejemplo, usuario1@midominio.com.
- Los usuarios que se encuentran en un dominio que no es un origen de identidad de vCenter Single Sign-On no pueden iniciar sesión en vCenter Server. Si el dominio que va a agregar a vCenter Single Sign-On forma parte de una jerarquía de dominios, Active Directory determinará si los usuarios de otros dominios de la jerarquía se autentican o no.

Si el entorno incluye una jerarquía de Active Directory, consulte el artículo 2064250 de la base de conocimientos de VMware para obtener detalles sobre las configuraciones compatibles y no compatibles.

Nota Se admite la autenticación de dos factores partir de vSphere 6.0 Update 2. Consulte Descripción de la autenticación de dos factores de vCenter Server.

Grupos del dominio de vCenter Single Sign-On

El dominio de vCenter Single Sign-On (vsphere.local de forma predeterminada) incluye varios grupos predefinidos. Agregue usuarios a uno de esos grupos para permitirles llevar a cabo las acciones correspondientes.

Consulte Administrar usuarios y grupos de vCenter Single Sign-On.

Para todos los objetos de la jerarquía de vCenter Server, puede asignar los permisos mediante el emparejamiento de un usuario y una función con el objeto. Por ejemplo, puede seleccionar un grupo de recursos y otorgar a un grupo de usuarios la función correspondiente para proporcionarle privilegios de lectura en ese objeto del grupo de recursos.

Para algunos servicios que vCenter Server no administra directamente, los privilegios se determinan por la pertenencia a uno de los grupos de vCenter Single Sign-On. Por ejemplo, un usuario que es miembro del grupo Administrador puede administrar vCenter Single Sign-On. Un usuario miembro del grupo Administradores de CA puede administrar VMware Certificate Authority y un usuario que está en el grupo Servicio de licencias.Administradores puede administrar licencias.

Los siguientes grupos están predefinidos en vsphere.local.

Nota Muchos de estos grupos son internos de vsphere.local u otorgan a los usuarios privilegios administrativos de alto nivel. Evalúe detenidamente los riesgos antes de agregar usuarios a cualquiera de estos grupos.

Nota No elimine ninguno de los grupos predefinidos en el dominio vsphere.local. De lo contrario, se pueden producir errores en la autenticación o el aprovisionamiento de certificados.

Tabla 2-1. Grupos del dominio vsphere.local

Privilegio	Descripción
Usuarios	Usuarios del dominio de vCenter Single Sign-On (vsphere.local de forma predeterminada).
Usuarios de solución	Servicios de vCenter del grupo de usuarios de solución. Cada usuario de solución se autentica de forma individual en vCenter Single Sign-On con un certificado. De forma predeterminada, VMCA aprovisiona a los usuarios de solución con certificados. No agregue miembros a este grupo explícitamente.
Administradores de CA	Miembros del grupo Administradores de CA que tienen privilegios de administrador para VMCA. No agregue miembros a este grupo a menos que tenga razones de peso para hacerlo.

Tabla 2-1. Grupos del dominio vsphere.local (continuación)

Privilegio	Descripción
Administradores de DC	Los miembros del grupo Administradores de DC pueden llevar a cabo acciones de administrador de la controladora de dominio en VMware Directory Service. **Nota** No administre la controladora de dominio directamente. En su lugar, utilice la CLI `vmdir` o vSphere Client para llevar a cabo las tareas correspondientes.
Configuración del sistema.Administradores de shell de Bash	Este grupo solo está disponible para implementaciones de vCenter Server Appliance. Un usuario de este grupo puede habilitar y deshabilitar el acceso al shell de BASH. De forma predeterminada, un usuario que se conecta a vCenter Server Appliance con SSH tiene acceso solo a los comandos del shell restringido. Los usuarios que están en este grupo pueden acceder al shell de BASH.
Actuar como usuarios	Los miembros del grupo Actuar como usuarios tienen permisos de obtención de tokens Actuar como de vCenter Single Sign-On.
Usuarios de IPDU externos	Este grupo interno no se utiliza en vSphere. VMware vCloud Air necesita este grupo.
Configuración del sistema.Administradores	Los miembros del grupo Configuración del sistema.Administradores pueden ver y administrar la configuración del sistema en vSphere Client. Estos usuarios pueden ver, iniciar y reiniciar servicios, solucionar problemas de los servicios, y ver y administrar los nodos disponibles.
Clientes de DC	Este grupo se utiliza internamente para permitir al nodo de administración acceder a los datos de VMware Directory Service. **Nota** No modifique este grupo. Cualquier cambio puede comprometer la infraestructura de certificados.
Administrador de componentes.Administradores	Los miembros del grupo Administrador de componentes.Administradores pueden ejecutar las API del administrador de componentes que registran servicios o cancelan registros de servicios, es decir, pueden modificar servicios. No es necesario ser miembro de este grupo para tener acceso de lectura en los servicios.
Servicio de licencias.Administradores	Los miembros de Servicio de licencias.Administradores tienen acceso total de escritura a todos los datos relacionados con la concesión de licencias, y pueden agregar, quitar y asignar claves de serie, así como anular estas asignaciones, para todos los activos de productos registrados en el servicio de concesión de licencias.
Administradores	Administradores de VMware Directory Service (vmdir). Los miembros de este grupo pueden realizar tareas de administración de vCenter Single Sign-On. No agregue miembros a este grupo a menos que tenga razones de peso para hacerlo y sepa cuáles son las consecuencias.

Configurar orígenes de identidad de vCenter Single Sign-On

Cuando un usuario inicia sesión solo con un nombre de usuario, vCenter Single Sign-On comprueba en el origen de identidad predeterminado si ese usuario puede autenticarse. Cuando un usuario inicia sesión e incluye el nombre de dominio en la pantalla de inicio de sesión, vCenter

Single Sign-On comprueba el dominio especificado si ese dominio se agregó como origen de identidad. Es posible agregar orígenes de identidad, quitar orígenes de identidad y cambiar el valor predeterminado.

vCenter Single Sign-On se configura desde vSphere Client. Para configurar vCenter Single Sign-On, se deben tener privilegios de administrador de vCenter Single Sign-On. Tener privilegios de administrador de vCenter Single Sign-On es diferente a tener función de administrador en vCenter Server o ESXi. En una nueva instalación, solo el administrador de vCenter Single Sign-On (administrator@vsphere.local de forma predeterminada) puede autenticarse en vCenter Single Sign-On.

- Orígenes de identidad para vCenter Server con vCenter Single Sign-On

  Puede utilizar orígenes de identidad para adjuntar uno o más dominios a vCenter Single Sign-On. Un dominio es un repositorio para usuarios y grupos que el servidor vCenter Single Sign-On puede utilizar para autenticación de usuarios.

- Establecer el dominio predeterminado de vCenter Single Sign-On

  Cada origen de identidad de vCenter Single Sign-On está asociado a un dominio. vCenter Single Sign-On utiliza el dominio predeterminado para autenticar a un usuario que inicia sesión sin un nombre de dominio. Los usuarios que pertenecen a un dominio que no es el predeterminado deben incluir el nombre de dominio para iniciar sesión.

- Agregar o editar un origen de identidad vCenter Single Sign-On

  Los usuarios pueden iniciar sesión en vCenter Server solo si están en un dominio que se agregó como origen de identidad de vCenter Single Sign-On. Los usuarios administradores de vCenter Single Sign-On pueden agregar orígenes de identidad o cambiar la configuración de los orígenes de identidad que agregaron.

- Usar vCenter Single Sign-On con autenticación de sesión de Windows

  Puede usar vCenter Single Sign-On con la autenticación de sesión de Windows (SSPI). Debe unir Platform Services Controller a un dominio de Active Directory antes de poder usar SSPI.

Orígenes de identidad para vCenter Server con vCenter Single Sign-On

Puede utilizar orígenes de identidad para adjuntar uno o más dominios a vCenter Single Sign-On. Un dominio es un repositorio para usuarios y grupos que el servidor vCenter Single Sign-On puede utilizar para autenticación de usuarios.

Los administradores pueden agregar orígenes de identidad, configurar el origen de identidad predeterminado y crear usuarios y grupos en el origen de identidad vsphere.local.

Los datos de usuarios y grupos se almacenan en Active Directory, OpenLDAP o localmente en el sistema operativo del equipo en el que está instalado vCenter Single Sign-On. Tras la instalación, todas las instancias de vCenter Single Sign-On tienen el origen de identidad *your_domain_name*; por ejemplo, vsphere.local. Este origen de identidad es interno de vCenter Single Sign-On.

Las versiones de vCenter Server anteriores a 5.1 eran compatibles con Active Directory y con usuarios del sistema operativo local como repositorios de usuarios. Como resultado, los usuarios del sistema operativo local siempre podían autenticarse en el sistema vCenter Server. Las versiones vCenter Server 5.1 y 5.5 utilizan vCenter Single Sign-On para la autenticación. Consulte la documentación de vSphere 5.1 para obtener una lista de orígenes de identidad compatibles con vCenter Single Sign-On 5.1. vCenter Single Sign-On 5.5 admite los siguientes tipos de repositorios de usuarios como orígenes de identidad, pero solo admite un origen de identidad predeterminado.

- Versiones de Active Directory 2003 y posteriores. Se muestran como **Active Directory (autenticación integrada de Windows)** en vSphere Client. vCenter Single Sign-On permite especificar un único dominio de Active Directory como origen de identidad. El dominio puede tener dominios secundarios o ser un dominio raíz del bosque. El artículo de la base de conocimientos de VMware 2064250 describe las confianzas de Microsoft Active Directory compatibles con vCenter Single Sign-On.
- Active Directory en LDAP. vCenter Single Sign-On admite varios orígenes de identidad de Active Directory en LDAP. Este tipo de origen de identidad se incluye para fines de compatibilidad con el servicio vCenter Single Sign-On que se ofrece con vSphere 5.1. Se muestra como **Active Directory como servidor LDAP** en vSphere Client.
- OpenLDAP versiones 2.4 y posteriores. vCenter Single Sign-On es compatible con varios orígenes de identidad de OpenLDAP. Se muestra como **OpenLDAP** en vSphere Client.
- Usuarios del sistema operativo local. Los usuarios del sistema operativo local son locales en el sistema operativo en que se ejecuta el servidor vCenter Single Sign-On. El origen de identidad del sistema operativo local solo existe en implementaciones del servidor vCenter Single Sign-On básicas y no está disponible en implementaciones con varias instancias de vCenter Single Sign-On. Solo se admite un origen de identidad del sistema operativo local. Se muestra como **localos** en vSphere Client.

  Nota No utilice los usuarios del sistema operativo local si Platform Services Controller se encuentra en un equipo diferente al del sistema vCenter Server. El empleo de usuarios del sistema operativo local podría tener sentido en una implementación integrada, pero no se recomienda.

- Usuarios del sistema vCenter Single Sign-On. Cuando se instala vCenter Single Sign-On, se crea exactamente un origen de identidad del sistema.

Nota En todo momento, solo hay un único dominio predeterminado. Si un usuario de un dominio que no es el predeterminado inicia sesión, debe agregar el nombre de dominio (*DOMAIN**user*) para poder autenticarse correctamente.

Establecer el dominio predeterminado de vCenter Single Sign-On

Cada origen de identidad de vCenter Single Sign-On está asociado a un dominio. vCenter Single Sign-On utiliza el dominio predeterminado para autenticar a un usuario que inicia sesión sin un

nombre de dominio. Los usuarios que pertenecen a un dominio que no es el predeterminado deben incluir el nombre de dominio para iniciar sesión.

Cuando un usuario inicia sesión en un sistema vCenter Server desde vSphere Client, el comportamiento de inicio de sesión depende de si el usuario se encuentra o no en el dominio configurado como el origen de identidad predeterminado.

- Los usuarios que están en el dominio predeterminado pueden iniciar sesión con su nombre de usuario y contraseña.
- Los usuarios que están en un dominio que se ha agregado a vCenter Single Sign-On como un origen de identidad, pero que no es el dominio predeterminado, pueden iniciar sesión en vCenter Server, pero deben especificar el dominio de una de las siguientes maneras.
  - Incluyendo un prefijo de nombre de dominio; por ejemplo, MIDOMINIO\usuario1.
  - Incluyendo el dominio; por ejemplo, usuario1@midominio.com.
- Los usuarios que se encuentran en un dominio que no es un origen de identidad de vCenter Single Sign-On no pueden iniciar sesión en vCenter Server. Si el dominio que va a agregar a vCenter Single Sign-On forma parte de una jerarquía de dominios, Active Directory determinará si los usuarios de otros dominios de la jerarquía se autentican o no.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en **Orígenes de identidad**, seleccione un origen de identidad y haga clic en **Establecer como predeterminado**.

   En la pantalla del dominio, el dominio predeterminado muestra la opción (predeterminado) en la columna Dominio.

Agregar o editar un origen de identidad vCenter Single Sign-On

Los usuarios pueden iniciar sesión en vCenter Server solo si están en un dominio que se agregó como origen de identidad de vCenter Single Sign-On. Los usuarios administradores de vCenter Single Sign-On pueden agregar orígenes de identidad o cambiar la configuración de los orígenes de identidad que agregaron.

Un origen de identidad puede ser un dominio de Active Directory nativo (autenticación integrada de Windows) o un servicio de directorio de OpenLDAP. Por razones de compatibilidad con versiones anteriores, Active Directory también está disponible como servidor LDAP. Consulte Orígenes de identidad para vCenter Server con vCenter Single Sign-On.

Inmediatamente después de la instalación, quedan disponibles los siguientes orígenes de identidad y usuarios predeterminados:

localos

Todos los usuarios locales del sistema operativo. Si va a realizar una actualización, los usuarios de `localos` que ya pueden autenticarse podrán seguir haciéndolo. El uso del origen de identidad de `localos` no funciona en los entornos que utilizan una instancia integrada de Platform Services Controller.

vsphere.local

Contiene los usuarios internos de vCenter Single Sign-On.

Requisitos previos

Si va a agregar un origen de identidad de Active Directory, vCenter Server Appliance o el equipo Windows en el cual se ejecuta vCenter Server deben estar en el dominio de Active Directory. Consulte Agregar un dispositivo de Platform Services Controller a un dominio de Active Directory.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en **Orígenes de identidad** y en **Agregar origen de identidad**.

5 Seleccione el origen de identidad e introduzca su configuración.

Opción	Descripción
Active Directory (autenticación integrada de Windows)	Utilice esta opción para las implementaciones nativas de Active Directory. Si desea utilizar esta opción, la máquina en la que se ejecuta el servicio vCenter Single Sign-On debe estar en un dominio de Active Directory. Consulte Configurar orígenes de identidad de Active Directory.
Active Directory en LDAP	Esta opción está disponible para brindar compatibilidad con versiones anteriores. Requiere que especifique la controladora de dominio y otra información. Consulte Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory.
OpenLDAP	Utilice esta opción para un origen de identidad OpenLDAP. Consulte Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory.
Sistema operativo local de servidor SSO	Utilice esta opción para el sistema operativo local del servidor SSO.

Nota Si se bloquea o se deshabilita la cuenta, las autenticaciones y las búsquedas de grupos y de usuarios en el dominio de Active Directory no funcionan. La cuenta del usuario debe tener acceso de solo lectura a la unidad organizativa del usuario y del grupo, y debe poder leer los atributos del usuario y del grupo. Active Directory ofrece este acceso de manera predeterminada. Utilice un usuario de servicio especial para obtener una mayor seguridad.

6 Haga clic en **Agregar**.

Pasos siguientes

Cuando se agrega un origen de identidad, todos los usuarios pueden autenticarse, pero tienen la función **Sin acceso**. Un usuario con privilegios de **Modify.permissions** de vCenter Server puede otorgar privilegios a usuarios o grupos de usuarios. Los privilegios permiten a los usuarios o grupos iniciar sesión en vCenter Server, así como ver y administrar objetos. Puede configurar permisos para que los usuarios y grupos de un dominio asociado de Active Directory puedan acceder a los componentes de vCenter Server. Consulte la documentación de *Seguridad de vSphere*.

Configurar orígenes de identidad de Active Directory

Si selecciona el tipo de origen de identidad de **Active Directory (autenticación de Windows integrada)**, puede usar la cuenta de equipo local como un nombre de entidad de seguridad de servicio (Service Principal Name, SPN) o especificar un SPN explícitamente. Puede usar esta opción únicamente si el servidor vCenter Single Sign-On está asociado a un dominio de Active Directory.

Requisitos previos para usar un origen de identidad de Active Directory

Puede configurar vCenter Single Sign-On para que use un origen de identidad de Active Directory solo si ese origen de identidad está disponible.

- Para una instalación de Windows, únase al equipo Windows en el dominio de Active Directory.
- Para vCenter Server Appliance, siga las instrucciones en la documentación de *Configuración de vCenter Server Appliance*.

Nota Active Directory (autenticación integrada de Windows) usa siempre la raíz del bosque de dominios de Active Directory. Para configurar un origen de identidad para Autenticación de Windows integrado con un dominio secundario dentro del bosque de Active Directory, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2070433.

Seleccione **Usar cuenta de equipo** para acelerar la configuración. Si desea cambiar el nombre del equipo local en el que se ejecuta vCenter Single Sign-On, es preferible que especifique un SPN explícitamente.

Nota En vSphere 5.5, vCenter Single Sign-On usa la cuenta del equipo aunque se especifique el SPN. Consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2087978.

Si habilitó el registro de eventos de diagnóstico en Active Directory para identificar dónde es posible que se necesite una protección, puede que vea un evento de registro con el identificador 2889 en ese servidor de directorio. El identificador de evento 2889 se genera como una anomalía en lugar de un riesgo de seguridad cuando se utiliza la autenticación integrada de Windows. Para obtener más información sobre el identificador de evento 2889, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/78644.

Tabla 2-2. Agregar opciones de orígenes de identidad

Cuadro de texto	Descripción
Nombre de dominio	FQDN del nombre de dominio (por ejemplo, midominio.com). No incluya una dirección IP. El sistema vCenter Server debe poder resolver este nombre de dominio mediante DNS. Si utiliza vCenter Server Appliance, use la información sobre la configuración de parámetros de red para actualizar la configuración del servidor DNS.
Usar cuenta de equipo	Seleccione esta opción para usar la cuenta de equipo local como el SPN. Si selecciona esta opción, solo debe especificar el nombre de dominio. No seleccione esta opción si desea cambiar el nombre de este equipo.
Usar nombre de entidad de seguridad de servicio (SPN)	Seleccione esta opción si desea cambiar el nombre del equipo local. Debe especificar un SPN, un usuario que pueda autenticarse con el origen de identidad y una contraseña para el usuario.

Tabla 2-2. Agregar opciones de orígenes de identidad (continuación)

Cuadro de texto	Descripción
Nombre de entidad de seguridad de servicio (SPN)	SPN ayuda a que Kerberos identifique el servicio de Active Directory. Incluya un dominio en el nombre (por ejemplo, `STS/ejemplo.com`). El SPN debe ser único en todo el dominio. La ejecución de `setspn -S` comprueba que no se creen duplicados. Consulte la documentación de Microsoft para obtener información sobre `setspn`.
Nombre principal de usuario (UPN) **Contraseña**	Nombre y contraseña de un usuario que puede autenticarse con este origen de identidad. Utilice el formato de dirección de correo electrónico (por ejemplo, `jchin@midominio.com`). Puede comprobar el nombre principal de usuario con el editor de interfaces del servicio de Active Directory (editor ADSI).

Configurar origen de identidad de servidores OpenLDAP y LDAP de Active Directory

El origen de identidad de Active Directory en LDAP es preferible a la opción de Active Directory (autenticación de Windows integrada). El origen de identidad de servidores OpenLDAP está disponible para los entornos que usan OpenLDAP.

Si planea configurar un origen de identidad de OpenLDAP, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2064977 para obtener información sobre los requisitos adicionales.

Nota Una actualización futura a Microsoft Windows cambiará el comportamiento predeterminado de Active Directory para exigir una autenticación y un cifrado seguros. Este cambio afectará al modo en que vCenter Server se autentica en Active Directory. Si utiliza Active Directory como origen de identidad para vCenter Server, debe tener previsto habilitar LDAP. Para obtener más información sobre esta actualización de seguridad de Microsoft, consulte https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 y https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Tabla 2-3. Configuración de servidores OpenLDAP y LDAP de Active Directory

Opción	Descripción
Nombre	Nombre del origen de identidad.
DN base para usuarios	El nombre distintivo base para los usuarios. Introduzca el DN desde el que se iniciarán las búsquedas de usuarios. Por ejemplo, cn=Users,dc=myCorp,dc=com.
DN base para grupos	El nombre distintivo base de los grupos. Introduzca el DN a partir del que se iniciarán las búsquedas de grupos. Por ejemplo, cn=Groups,dc=myCorp,dc=com.
Nombre de dominio	El nombre de dominio completo.

Tabla 2-3. Configuración de servidores OpenLDAP y LDAP de Active Directory (continuación)

Opción	Descripción
Alias de dominio	Para los orígenes de identidad de Active Directory, el nombre de NetBIOS del dominio. Si usa autenticaciones de SSPI, agregue el nombre de NetBIOS del dominio de Active Directory como alias del origen de identidad. Para los orígenes de identidad de OpenLDAP, si no se especifica un alias, se agrega el nombre del dominio en mayúsculas.
Nombre de usuario	Identificador de un usuario del dominio que tiene, como mínimo, acceso de solo lectura al DN base para los usuarios y los grupos. El identificador puede tener cualquiera de estos formatos: ■ UPN (usuario@dominio.com) ■ NetBIOS (DOMINIO\usuario) ■ DN (cn=usuario,cn=Usuarios,dc=dominio,dc=com) El nombre de usuario debe ser completo. Una entrada de "usuario" no funciona.
Contraseña	Contraseña del usuario especificado en el campo **Nombre de usuario**.
Conectar con	Controladora de dominio a la cual conectarse. Puede ser cualquier controladora de dominio en el dominio o controladoras específicas.
URL de servidor principal	El servidor LDAP de la controladora de dominio principal para el dominio. Use el formato **`ldap://nombre de host o dirección IP:puerto`** o **`ldaps://nombre de host o dirección IP:puerto`**. Por lo general, el puerto es el 389 para las conexiones de LDAP y 636 para las conexiones de LDAPS. Para las implementaciones de controladoras de varios dominios de Active Directory, el puerto suele ser el 3268 para las conexiones de LDAP y el 3269 para las conexiones de LDAPS. Se necesita un certificado que establezca la confianza para el endpoint de LDAPS del servidor Active Directory cuando se usa **`ldaps://`** en la dirección URL del servidor LDAP principal o secundario.
URL de servidor secundario	Dirección de un servidor LDAP de controladora de dominio secundario que se usa para la conmutación por error.
certificados SSL	Si desea utilizar LDAPS con el servidor de LDAP de Active Directory o el origen de identidad del servidor OpenLDAP, haga clic en **`Examinar`** para elegir un certificado. Para exportar el certificado de CA raíz de Active Directory, consulte la documentación de Microsoft.

Usar vCenter Single Sign-On con autenticación de sesión de Windows

Puede usar vCenter Single Sign-On con la autenticación de sesión de Windows (SSPI). Debe unir Platform Services Controller a un dominio de Active Directory antes de poder usar SSPI.

El uso de SSPI acelera el proceso de inicio de sesión del usuario que tiene una sesión abierta en una máquina.

Requisitos previos

- Una el dispositivo de Platform Services Controller o la máquina de Windows en la que esté ejecutándose Platform Services Controller a un dominio de Active Directory. Consulte Agregar un dispositivo de Platform Services Controller a un dominio de Active Directory.
- Compruebe que el dominio esté configurado correctamente. Consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2064250.
- Si está usando vSphere 6.0 o una versión anterior, compruebe que el complemento de integración de clientes esté instalado.
- Si está usando vSphere 6.5 o una versión posterior, compruebe que el complemento de autenticación mejorado esté instalado. Consulte *Instalar y configurar vCenter Server*.

Procedimiento

1. Desplácese hasta la página de inicio de sesión de vSphere Client.
2. Active la casilla **Usar la autenticación de sesión de Windows**.
3. Inicie sesión usando el nombre de usuario y la contraseña de Active Directory.
   - Si el dominio de Active Directory es el origen de identidad predeterminado, inicie sesión con su nombre de usuario, por ejemplo, jlee.
   - De lo contrario, incluya el nombre de dominio, por ejemplo, jlee@example.com.

Descripción de la autenticación de dos factores de vCenter Server

vCenter Single Sign-On le permite autenticarse como usuario en un origen de identidad que vCenter Single Sign-On conoce, o bien mediante la autenticación de sesión de Windows. También puede autenticarse a través de una tarjeta inteligente (tarjeta de acceso común —Common Access Card, CAC— basada en UPN) o mediante un token RSA SecurID.

Métodos de autenticación de dos factores

Los métodos de autenticación de dos factores a menudo son requeridos por agencias gubernamentales o empresas de gran tamaño.

Autenticación de tarjeta inteligente

La autenticación de tarjeta inteligente solo permite el acceso a usuarios que adjuntan una tarjeta física a la unidad USB del equipo donde inician sesión. Un ejemplo es la autenticación de tarjeta de acceso común (Common Access Card, CAC).

El administrador puede implementar la PKI para que los certificados de tarjeta inteligente sean los únicos certificados de cliente que emita la CA. En estas implementaciones, al usuario solo se le presentan certificados de tarjeta inteligente. El usuario selecciona un certificado y se le solicita un PIN. Solo los usuarios que tienen tarjeta física y el PIN que coincide con el certificado pueden iniciar sesión.

Autenticación de RSA SecurID

Para utilizar la autenticación de RSA SecurID, el entorno debe incluir una instancia de RSA Authentication Manager configurada correctamente. Si Platform Services Controller está configurado para apuntar al servidor RSA, y si la autenticación de RSA SecurID está habilitada, los usuarios pueden iniciar sesión con su nombre de usuario y su token.

Para obtener más información, consulte las dos publicaciones del blog de vSphere sobre la configuración de RSA SecurID.

Nota vCenter Single Sign-On solo admite SecurID nativo. No admite autenticación RADIUS.

Especificar un método de autenticación no predeterminado

Los administradores pueden configurar un método de autenticación no predeterminado en vSphere Client o mediante el script `sso-config`.

- Para la autenticación de tarjeta inteligente, puede realizar la configuración de vCenter Single Sign-On desde vSphere Client o mediante `sso-config`. La configuración incluye la habilitación de la autenticación de tarjetas inteligentes y la configuración de las políticas de revocación de certificados.
- En el caso de RSA SecurID, puede utilizar el script `sso-config` para configurar RSA Authentication Manager para el dominio y para habilitar la autenticación de token de RSA. La autenticación de RSA SecurID no puede configurarse desde vSphere Client. Sin embargo, si habilita RSA SecurID, ese método de autenticación aparece en vSphere Client.

Combinar métodos de autenticación

Los métodos de autenticación se pueden habilitar o deshabilitar de forma separada utilizando `sso-config`. Inicialmente, deje habilitada la autenticación por nombre de usuario y contraseña mientras prueba un método de autenticación de dos factores; después de las pruebas, habilite un único método de autenticación.

Inicio de sesión de autenticación de tarjeta inteligente

Una tarjeta inteligente es una tarjeta plástica pequeña con un chip de circuito integrado. Muchas agencias gubernamentales y empresas grandes utilizan tarjetas inteligentes como tarjetas de acceso común (CAC) para incrementar la seguridad de los sistemas y cumplir con las normas

de seguridad. Se utiliza una tarjeta inteligente en aquellos entornos donde todas las máquinas incluyen un lector para este tipo de tarjetas. Los controladores del hardware de tarjetas inteligentes que las gestionan suelen estar preinstalados.

A los usuarios que inician sesión en un sistema vCenter Server o Platform Services Controller se les pide que realicen la autenticación con una combinación de tarjeta inteligente y PIN, como se indica a continuación.

1 Cuando se introduce la tarjeta inteligente en el lector de tarjetas inteligentes, vCenter Single Sign-On lee los certificados en la tarjeta.
2 vCenter Single Sign-On solicita al usuario que seleccione un certificado y luego solicita el PIN correspondiente a dicho certificado.
3 vCenter Single Sign-On verifica si el certificado de la tarjeta inteligente es conocido y si el PIN es correcto. Si la verificación de revocación está activa, vCenter Single Sign-On también verifica si el certificado fue revocado.
4 Si el certificado es conocido y no es un certificado revocado, el usuario es autenticado y puede realizar las tareas para las que tiene permisos.

Nota Generalmente, es lógico dejar la autenticación por nombre y contraseña activada durante las pruebas. Una vez completada la prueba, deshabilite la autenticación por nombre de usuario y contraseña, y habilite la autenticación de tarjeta inteligente. Posteriormente, vSphere Client y vSphere Web Client permiten solo el inicio de sesión de tarjeta inteligente. Solo los usuarios con privilegios de raíz o administrador en la máquina podrán volver a habilitar la autenticación por nombre de usuario y contraseña iniciando sesión directamente en Platform Services Controller.

Configurar y usar la autenticación de tarjeta inteligente

El entorno puede configurarse para que se requiera autenticación de tarjeta inteligente cuando un usuario se conecta a vCenter Server o una instancia de Platform Services Controller asociada desde vSphere Client o vSphere Web Client.

La forma de configurar la autenticación de tarjeta inteligente depende de la versión de vSphere que se utilice.

Versión de vSphere	Procedimiento	Vínculos
6.0 Update 2 Versiones posteriores de vSphere 6.0	1 Configure el servidor Tomcat. 2 Habilite y configure la autenticación de tarjeta inteligente.	Centro de documentación de vSphere 6.0.
6.5 y posteriores	1 Configure el proxy inverso. 2 Habilite y configure la autenticación de tarjeta inteligente.	Configurar el proxy inverso para solicitar certificados de clientes Usar la línea de comandos para administrar la autenticación de tarjeta inteligente Administrar la autenticación de tarjeta inteligente

Configurar el proxy inverso para solicitar certificados de clientes

Antes de habilitar la autenticación de la tarjeta inteligente, debe configurar el proxy inverso en el sistema de Platform Services Controller. Si su entorno utiliza un Platform Services Controller integrado, debe realizar estar tarea en el sistema en el que se ejecutan tanto vCenter Server como Platform Services Controller.

Se necesita una configuración de proxy inverso en vSphere 6.5 y posteriores.

Requisitos previos

Copie los certificados de CA al sistema de Platform Services Controller.

Procedimiento

1 Inicie sesión en Platform Services Controller.

Sistema operativo	Descripción
Dispositivo	Inicie sesión en el shell del dispositivo como usuario raíz.
Windows	Inicie sesión en el símbolo del sistema de Windows como usuario administrador.

2 Cree un almacén de CA de un cliente de confianza.

Este almacén contendrá los certificados de la CA emisora de confianza para el certificado de cliente. El cliente aquí es el explorador desde el que el proceso de la tarjeta inteligente solicita información al usuario final.

El siguiente ejemplo muestra cómo crear un almacén de certificados en el dispositivo de Platform Services Controller.

Para un único certificado:

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-
sts/conf/clienttrustCA.pem
```

Para varios certificados:

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/
vmware-sts/conf/clienttrustCA.pem
```

Nota En Platform Services Controller en Windows, utilice `C:\ProgramData\VMware\vCenterServer\runtime\VMwareSTSService\conf\` y cambie el comando para que utilice la barra invertida.

3 Cree una copia de seguridad del archivo `config.xml` que incluya la definición del proxy inverso y abra `config.xml` en un editor.

Sistema operativo	Descripción
Dispositivo	`/etc/vmware-rhttpproxy/config.xml`
Windows	`C:\ProgramData\VMware\vCenterServer\cfg\vmware-rhttpproxy\config.xml`

4 Realice los siguientes cambios y guarde el archivo.

```
<http>
<maxConnections> 2048 </maxConnections>
<requestClientCertificate>true</requestClientCertificate>
<clientCertificateMaxSize>4096</clientCertificateMaxSize>
<clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
</http>
```

El archivo `config.xml` incluye algunos de estos elementos. Quite las marcas de comentarios de los elementos, actualice los elementos o agréguelos según sea necesario.

5 Reinicie el servicio.

Sistema operativo	Descripción
Dispositivo	`/usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy`
Windows	Reinicie el sistema operativo o bien reinicie VMware HTTP Reverse Proxy siguiendo los pasos que se indican a continuación: a Abra un símbolo del sistema con privilegios elevados. b Ejecute los siguientes comandos: `cd C:\Program Files\VMware\vCenter Server\bin` `service-control --stop vmware-rhttpproxy` `service-control --start vmware-rhttpproxy`

Usar la línea de comandos para administrar la autenticación de tarjeta inteligente

La utilidad `sso-config` se puede utilizar para administrar la autenticación de tarjeta inteligente desde la línea de comandos. La utilidad admite todas las tareas de configuración de tarjeta inteligente.

Puede encontrar el script de `sso-config` en las siguientes ubicaciones:

Windows	`C:\Archivos de programa\VMware\VCenter server\VMware Identity Services\sso-config.bat`
Linux	`/opt/vmware/bin/sso-config.sh`

La configuración de los tipos de autenticación admitidos y la configuración de revocación se almacenan en VMware Directory Service y se replican en todas las instancias de Platform Services Controller en un dominio de vCenter Single Sign-On.

Si se deshabilita la autenticación con nombre de usuario y contraseña, y si hay problemas con la autenticación de tarjeta inteligente, los usuarios no podrán iniciar sesión. En ese caso, un usuario raíz o un usuario administrador pueden activar la autenticación con nombre de usuario y contraseña en la línea de comandos de Platform Services Controller. El siguiente comando habilita la autenticación con nombre de usuario y contraseña.

Sistema operativo	Comando
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` Si utiliza el tenant predeterminado, use vsphere.local como nombre de tenant.
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` Si utiliza el tenant predeterminado, use vsphere.local como nombre de tenant.

Si utiliza OCSP para la comprobación de revocación, puede basarse en el OCSP predeterminado que se especificó en la extensión AIA del certificado de tarjeta inteligente. También se puede anular la opción predeterminada y configurar uno o más respondedores OCSP alternativos. Por ejemplo, se pueden configurar respondedores OCSP locales en el sitio de vCenter Single Sign-On para procesar la solicitud de comprobación de revocación.

Nota Si el certificado no tiene un OCSP definido, habilite en cambio la CRL (lista de revocación de certificados).

Requisitos previos

- Compruebe que el entorno utilice la versión 6.5 de Platform Services Controller o versiones posteriores y que se esté utilizando la versión 6.0 de vCenter Server o versiones posteriores. La versión 6.0 Update 2 de Platform Services Controller admite la autenticación de tarjeta inteligente, pero el procedimiento de configuración es diferente.
- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (Public Key Infrastructure, PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (User Principal Name, UPN) debe corresponder a una cuenta de Active Directory en la extensión del nombre alternativo del firmante (Subject Alternative Name, SAN).
  - El certificado debe especificar la autenticación del cliente en los campos Directiva de aplicación o Uso mejorado de claves; de lo contrario, el explorador no mostrará el certificado.

- Compruebe que el certificado de Platform Services Controller sea de confianza para la instancia de Workstation del usuario final. De lo contrario, el explorador no intentará la autenticación.
- Agregue un origen de identidad de Active Directory a vCenter Single Sign-On.
- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Posteriormente, esos usuarios pueden realizar tareas de autenticación debido a que poseen privilegios de administrador de vCenter Server.

Nota El administrador del dominio de vCenter Single Sign-On (de manera predeterminada, administrator@vsphere.local) no puede realizar la autenticación de tarjeta inteligente.

- Configure el proxy inverso y reinicie el equipo físico o la máquina virtual.

Procedimiento

1 Obtenga los certificados y cópielos en una carpeta que la utilidad `sso-config` pueda ver.

Opción	Descripción
Windows	Inicie sesión en la instancia de Platform Services Controller de la instalación de Windows y utilice WinSCP o una utilidad similar para copiar los archivos.
Dispositivo	a Inicie sesión en la consola de dispositivos, ya sea directamente o a través de SSH. b Habilite el shell del dispositivo, como se indica a continuación. `shell` `chsh -s "/bin/bash" root` c Utilice WinSCP o una utilidad similar para copiar los certificados en `/usr/lib/vmware-sso/vmware-sts/conf` en la instancia de Platform Services Controller. d Opcionalmente, deshabilite el shell del dispositivo, como se indica a continuación. `chsh -s "/bin/appliancesh" root`

2 Para habilitar la autenticación de tarjeta inteligente para VMware Directory Service (vmdir), ejecute el siguiente comando.

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
```

Por ejemplo:

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
MySmartCA1.cer,MySmartCA2.cer  -t vsphere.local
```

Separe los distintos certificados con comas, pero no incluya espacios después de la coma.

3 Para deshabilitar todos los otros métodos de autenticación, ejecute los siguientes comandos.

```
sso-config.[bat|sh] -set_authn_policy -pwdAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
```

4 (opcional) Para establecer una lista blanca de directivas de certificado, ejecute el siguiente comando.

```
sso-config.[bat|sh] -set_authn_policy -certPolicies policies
```

Para especificar varias directivas, sepárelas con una coma, por ejemplo:

```
sso-config.bat -set_authn_policy -certPolicies
2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
```

La lista blanca especifica los identificadores de objeto de las directivas que están permitidas en la extensión de directiva de certificados del certificado. Los certificados X509 pueden tener una extensión de directiva de certificados.

5 (opcional) Active y configure la comprobación de revocación mediante OCSP.

a Active la comprobación de revocación mediante OCSP.

```
sso-config.[bat|sh]  -set_authn_policy -t tenantName  -useOcsp true
```

b Si el vínculo del respondedor OCSP no se proporciona mediante la extensión AIA de los certificados, proporcione la URL del respondedor OCSP de anulación y el certificado de autoridad de OCSP.

El OCSP alternativo se configura para cada sitio de vCenter Single Sign-On. Es posible especificar más de un respondedor OCSP alternativo para el sitio de vCenter Single Sign-On de modo que permita la conmutación por error.

```
sso-config.[bat|sh] -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl
http://ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

Nota La configuración se aplica al sitio actual de vCenter Single Sign-On de forma predeterminada. Especifique el parámetro `siteID` únicamente si se configura un OCSP alternativo para otros sitios de vCenter Single Sign-On.

Tenga en cuenta el ejemplo siguiente:

```
 .sso-config.[bat|sh] -t vsphere.local -add_alt_ocsp
-ocspUrl http://failover.ocsp.nsn0.rcvs.nit.disa.mil/ -ocspSigningCert ./
DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP responder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c Para mostrar la configuración del respondedor OCSP alternativo actual, ejecute este comando.

```
sso-config.[bat|sh] -t tenantName -get_alt_ocsp]
```

d Para quitar la configuración del respondedor OCSP alternativo actual, ejecute este comando.

```
sso-config.[bat|sh] -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 (opcional) Para hacer una lista de la información de configuración, ejecute el siguiente comando.

```
sso-config.[bat|sh] -get_authn_policy -t tenantName
```

Administrar la autenticación de tarjeta inteligente

Puede habilitar o deshabilitar la autenticación de tarjeta inteligente, personalizar el banner de inicio de sesión y configurar la directiva de revocación desde vSphere Client.

Si se habilita la autenticación de tarjeta inteligente y se deshabilitan otros métodos de autenticación, se solicitará a los usuarios que inicien sesión con la autenticación de tarjeta inteligente.

Si se deshabilita la autenticación con nombre de usuario y contraseña, y si hay problemas con la autenticación de tarjeta inteligente, los usuarios no podrán iniciar sesión. En ese caso, un usuario raíz o un usuario administrador pueden activar la autenticación con nombre de usuario y contraseña en la línea de comandos de Platform Services Controller. El siguiente comando habilita la autenticación con nombre de usuario y contraseña.

Sistema operativo	Comando
Windows	sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name> Si utiliza el tenant predeterminado, use vsphere.local como nombre de tenant.
Linux	sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name> Si utiliza el tenant predeterminado, use vsphere.local como nombre de tenant.

Requisitos previos

- Compruebe que el entorno utilice la versión 6.5 de Platform Services Controller o versiones posteriores y que se esté utilizando la versión 6.0 de vCenter Server o versiones posteriores. La versión 6.0 Update 2 de Platform Services Controller admite la autenticación de tarjeta inteligente, pero el procedimiento de configuración es diferente.
- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (Public Key Infrastructure, PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (User Principal Name, UPN) debe corresponder a una cuenta de Active Directory en la extensión del nombre alternativo del firmante (Subject Alternative Name, SAN).

- El certificado debe especificar la autenticación del cliente en los campos Directiva de aplicación o Uso mejorado de claves; de lo contrario, el explorador no mostrará el certificado.

- Compruebe que el certificado de Platform Services Controller sea de confianza para la instancia de Workstation del usuario final. De lo contrario, el explorador no intentará la autenticación.
- Agregue un origen de identidad de Active Directory a vCenter Single Sign-On.
- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Posteriormente, esos usuarios pueden realizar tareas de autenticación debido a que poseen privilegios de administrador de vCenter Server.

  Nota El administrador del dominio de vCenter Single Sign-On (de manera predeterminada, administrator@vsphere.local) no puede realizar la autenticación de tarjeta inteligente.

- Configure el proxy inverso y reinicie el equipo físico o la máquina virtual.

Procedimiento

1 Obtenga los certificados y cópielos en una carpeta que la utilidad `sso-config` pueda ver.

Opción	Descripción
Windows	Inicie sesión en la instancia de Platform Services Controller de la instalación de Windows y utilice WinSCP o una utilidad similar para copiar los archivos.
Dispositivo	a Inicie sesión en la consola de dispositivos, ya sea directamente o a través de SSH. b Habilite el shell del dispositivo, como se indica a continuación. `shell` `chsh -s "/bin/bash" root` `csh -s "bin/appliance/sh" root` c Utilice WinSCP o una utilidad similar para copiar los certificados en `/usr/lib/vmware-sso/vmware-sts/conf` en la instancia de Platform Services Controller. d Opcionalmente, deshabilite el shell del dispositivo, como se indica a continuación. `chsh -s "/bin/appliancesh" root`

2 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

3 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

4 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

5 En **Autenticación de tarjeta inteligente**, haga clic en **Editar**.

6 Seleccione o anule la selección de los métodos de autenticación y haga clic en **Guardar**.

   Puede elegir la autenticación de tarjeta inteligente sola o la autenticación de tarjeta inteligente junto con la autenticación de sesión Windows y con contraseña.

   No puede habilitar o deshabilitar la autenticación de RSA SecurID desde esta interfaz web. Sin embargo, si se habilitó RSA SecurID desde la línea de comandos, el estado aparece en la interfaz web.

   Se mostrará **Certificados de CA de confianza**.

7 En la pestaña **Certificados de CA de confianza**, haga clic en **Agregar** y seleccione **Examinar**.

8 Seleccione todos los certificados de CA de confianza y haga clic en **Agregar**.

Pasos siguientes

El entorno puede requerir una configuración de OCSP mejorada.

- Si la respuesta OCSP es emitida por una CA distinta de la CA firmante de la tarjeta inteligente, proporcione el certificado de CA de firma correspondiente a OCSP.
- Puede configurar uno o más respondedores OCSP locales para cada sitio de Platform Services Controller en una implementación de varios sitios. Es posible configurar estos respondedores OCSP alternativos mediante la CLI. Consulte Usar la línea de comandos para administrar la autenticación de tarjeta inteligente.

Configurar directivas de revocación para autenticación de tarjeta inteligente

Puede personalizar la verificación de revocación de certificados, así como especificar en qué lugar vCenter Single Sign-On busca información sobre certificados revocados.

Puede personalizar el comportamiento utilizando vSphere Client o el script de `sso-config`. La configuración seleccionada depende en parte de lo que la CA admite.

- Si la verificación de revocación está deshabilitada, vCenter Single Sign-On ignora cualquier configuración de CRL o OCSP. vCenter Single Sign-On no realiza comprobaciones sobre ningún certificado.
- Si la verificación de revocación está habilitada, la configuración recomendada depende de la configuración de la PKI.

   Solo OCSP

   Si la CA emisora admite un respondedor OCSP, habilite **OCSP** y deshabilite **CRL como conmutación por error para OCSP**.

   Solo CRL

Si la CA emisora no admite OSCP, habilite la **verificación de CRL** y deshabilite la **verificación de OSCP**.

Tanto OSCP como CRL

Si la CA emisora admite tanto un respondedor OCSP como CRL, vCenter Single Sign-On verifica el respondedor OCSP primero. Si el respondedor devuelve un estado desconocido o no está disponible, vCenter Single Sign-On verifica la CRL primero. En este caso, habilite la **verificación de OCSP** y la **verificación de CRL**, y habilite **CRL como conmutación por error para OCSP**.

- Si la verificación de revocación está habilitada, los usuarios avanzados pueden especificar la siguiente configuración adicional.

  URL de OSCP

  De forma predeterminada, vCenter Single Sign-On verifica la ubicación del respondedor OCSP que se define en el certificado que se está validando. Si la extensión de acceso a la información de entidad no está presente en el certificado o si desea anularla, puede especificar explícitamente una ubicación.

  Usar CRL del certificado

  De forma predeterminada, vCenter Single Sign-On verifica la ubicación de CRL que se define en el certificado que se está validando. Deshabilite esta opción si el certificado no incluye la extensión del punto de distribución de CRL o si desea anular la que se define de forma predeterminada.

  Ubicación de CRL

  Utilice esta propiedad si deshabilita **Usar CRL del certificado** y desea especificar una ubicación (archivo o URL HTTP) en donde se encuentra la CRL.

Puede agregar una directiva de certificados para limitar aún más los certificados que acepta vCenter Single Sign-On.

Requisitos previos

- Compruebe que el entorno utilice la versión 6.5 de Platform Services Controller o versiones posteriores y que se esté utilizando la versión 6.0 de vCenter Server o versiones posteriores. La versión 6.0 Update 2 de Platform Services Controller admite la autenticación de tarjeta inteligente, pero el procedimiento de configuración es diferente.
- Compruebe que en su entorno se haya configurado una infraestructura de clave pública (Public Key Infrastructure, PKI) empresarial, y que los certificados cumplan con los siguientes requerimientos:
  - Un nombre principal de usuario (User Principal Name, UPN) debe corresponder a una cuenta de Active Directory en la extensión del nombre alternativo del firmante (Subject Alternative Name, SAN).

  - El certificado debe especificar la autenticación del cliente en los campos Directiva de aplicación o Uso mejorado de claves; de lo contrario, el explorador no mostrará el certificado.

- Compruebe que el certificado de Platform Services Controller sea de confianza para la estación de trabajo del usuario final. De lo contrario, el explorador no intentará la autenticación.
- Agregue un origen de identidad de Active Directory a vCenter Single Sign-On.
- Asigne la función de Administrador de vCenter Server a uno o más usuarios en el origen de identidad de Active Directory. Posteriormente, esos usuarios pueden realizar tareas de autenticación debido a que poseen privilegios de administrador de vCenter Server.

  Nota El administrador del dominio de vCenter Single Sign-On (de manera predeterminada, administrator@vsphere.local) no puede realizar la autenticación de tarjeta inteligente.

Procedimiento

1. Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.
2. Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.
3. Desplácese hasta la interfaz de usuario de configuración.
   a. En el menú **Inicio**, seleccione **Administración**.
   b. En **Single Sign On**, haga clic en **Configuración**.
4. Haga clic en **Autenticación de tarjeta inteligente**.
5. Haga clic en **Revocación de certificado** y haga clic en **Editar** para habilitar o deshabilitar la comprobación de revocación.
6. Si en su entorno hay directivas de certificados vigentes, puede agregar una directiva en el panel **Directivas de certificado**.

Configurar la autenticación de RSA SecurID

Se puede configurar el entorno de manera que se solicite a los usuarios iniciar sesión con un token RSA SecurID. La configuración de SecurID solo es compatible desde la línea de comandos.

Para obtener más información, consulte las dos publicaciones del blog de vSphere sobre la configuración de RSA SecurID.

Nota RSA Authentication Manager requiere que el identificador de usuario sea único, y que utilice entre 1 y 255 caracteres ASCII. Los caracteres Y comercial (&), porcentaje (%), mayor que (>), menor que (<) y apóstrofo (`) no están permitidos.

Requisitos previos

- Al configurar RSA SecurID, vCenter Single Sign-On (SSO) admite el uso del nombre principal de usuario (atributo userPrincipalName) como el identificador de usuario solo cuando la autenticación integrada de Windows (Integrated Windows Authentication, IWA) está configurada como un origen de identidad para los usuarios de RSA.
- Compruebe que el entorno utilice la versión 6.5 de Platform Services Controller o versiones posteriores y que se esté utilizando la versión 6.0 de vCenter Server o versiones posteriores. La versión 6.0 Update 2 de Platform Services Controller admite la autenticación de tarjeta inteligente, pero el procedimiento de configuración es diferente.
- Compruebe que RSA Authentication Manager se haya configurado correctamente en el entorno y que los usuarios disponen de tokens RSA.Compruebe que RSA Authentication Manager se haya configurado correctamente en el entorno y que los usuarios dispongan de tokens RSA. Se requiere RSA Authentication Manager versión 8.0 o posterior.
- Compruebe que el origen de identidad que utiliza RSA Manager se haya agregado a vCenter Single Sign-On. Consulte Agregar o editar un origen de identidad vCenter Single Sign-On.
- Compruebe que el sistema RSA Authentication Manager pueda resolver el nombre de host de Platform Services Controller y que el sistema Platform Services Controller pueda resolver el nombre de host de RSA Authentication Manager.
- Exporte el archivo `sdconf.rec` desde la instancia de RSA Manager seleccionando **Acceso > Agentes de autenticación > Generar archivo de configuración**. Descomprima el archivo `AM_Config.zip` resultante para buscar el archivo `sdconf.rec`.
- Copie el archivo `sdconf.rec` en el nodo Platform Services Controller.

Procedimiento

1 Pase al directorio donde se ubica el script de `sso-config`.

Opción	Descripción
Windows	`C:\Archivos de programa\VMware\VCenter server\VMware Identity Services`
Dispositivo	`/opt/vmware/bin`

2 Para habilitar la autenticación de RSA SecurID, ejecute el siguiente comando.

```
sso-config.[sh|bat]  -t tenantName  -set_authn_policy -securIDAuthn true
```

tenantName es el nombre del dominio vCenter Single Sign-On, vsphere.local de forma predeterminada.

3 (opcional) Para deshabilitar otros métodos de autenticación, ejecute el siguiente comando.

```
sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t
vsphere.local
```

4 Para configurar el entorno de forma que el tenant del sitio actual utilice el sitio de RSA, ejecute el siguiente comando.

```
sso-config.[sh|bat] -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-sdConfFile Path]
```

Por ejemplo:

```
sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
```

Puede especificar las siguientes opciones.

Opción	Descripción
siteID	Identificador opcional del sitio de Platform Services Controller. Platform Services Controller admite una instancia de RSA Authentication Manager o clúster por sitio. Si no especifica esta opción de manera explícita, la configuración de RSA se destina al sitio de Platform Services Controller actual. Solo utilice esta opción si desea agregar un sitio diferente.
agentName	Definido en RSA Authentication Manager.
sdConfFile	Copia del archivo `sdconfig.rec` que se descargó de RSA Manager, el cual incluye la información de configuración de RSA Manager (por ejemplo, la dirección IP).

5 (opcional) Para cambiar la configuración del tenant para que utilice valores distintos a los predeterminados, ejecute el siguiente comando.

```
sso-config.[sh|bat] -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size] [-maxLogFileCount Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList Alg1,Alg2,...]
```

El valor predeterminado suele ser adecuado, por ejemplo:

```
sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
```

6 (opcional) Si el origen de identidad no utiliza el nombre principal de usuario como identificador del usuario, configure el atributo userID del origen de identidad. (Compatible solo con orígenes de identidad de Active Directory en LDAP).

El atributo userID determina qué atributo LDAP se utiliza como userID en RSA.

```
sso-config.[sh|bat] -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr AttrName] [-siteID Location]
```

Por ejemplo:

```
sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr userPrincipalName
```

7 Para mostrar la configuración actual, ejecute el siguiente comando.

```
sso-config.sh -t tenantName -get_rsa_config
```

Resultados

Si la autenticación por nombre de usuario y contraseña no está habilitada, pero la autenticación de RSA sí lo está, los usuarios deben iniciar sesión con el nombre de usuario y el token RSA. Ya no es posible iniciar sesión con el nombre de usuario y la contraseña.

Nota Use el formato de nombre de usuario ***userID@domainName*** o ***userID@domain_upn_suffix***.

Administrar el mensaje de inicio de sesión

Puede incluir un mensaje de inicio de sesión con el entorno. Se puede habilitar o deshabilitar el mensaje de inicio de sesión, y se puede solicitar que los usuarios hagan clic en una casilla de consentimiento explícito.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

a En el menú **Inicio**, seleccione **Administración**.

b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en la pestaña **Mensaje de inicio de sesión**.

5 Haga clic en **Editar** y configure el mensaje de inicio de sesión.

Opción	Descripción
Mostrar mensaje de inicio de sesión	Alterne **Mostrar el mensaje de inicio de sesión** para habilitar el mensaje de inicio de sesión. No se pueden realizar cambios en el mensaje de inicio de sesión a menos que alterne este conmutador.
Mensaje de inicio de sesión	Título del mensaje. De forma predeterminada, cuando se alterna la **casilla de consentimiento**, el texto del mensaje de inicio de sesión es `I agree to Terms and Conditions`. Debe reemplazar `Terms and Conditions` con su propio texto. Si la **Casilla de verificación de consentimiento** está desactivada, a continuación aparece `Login message` donde deberá escribir el mensaje.

Opción	Descripción
Casilla de consentimiento	Alterne la **casilla de consentimiento** para requerir que el usuario haga clic en una casilla antes de iniciar sesión. También se puede mostrar un mensaje sin ninguna casilla.
Detalles del mensaje de inicio de sesión	Mensaje que ve el usuario cuando hace clic en el mensaje de inicio de sesión, por ejemplo, el texto de los términos y las condiciones. Debe introducir algunos detalles en este cuadro de texto.

6 Haga clic en **Guardar**.

Utilizar vCenter Single Sign-On como el proveedor de identidad para otro proveedor de servicios

vSphere Web Client se registra automáticamente como proveedor de servicios (Service Provider, SP) SAML 2.0 de confianza en vCenter Single Sign-On. Puede agregar otros proveedores de servicios de confianza a una federación de identidades en la que vCenter Single Sign-On actúe como proveedor de identidad (Identity Provider, IDP) SAML. Los proveedores de servicios deben cumplir con el protocolo SAML 2.0. Tras configurar la federación, el proveedor de servicios permite el acceso a un usuario si este puede autenticarse en vCenter Single Sign-On.

Nota vCenter Single Sign-On puede ser el IDP para otros SP.vCenter Single Sign-On no puede ser un SP que use otro IDP.

Un proveedor de servicios SAML registrado puede permitir el acceso a otro usuario que ya tenga una sesión activa, es decir, un usuario que haya iniciado sesión en el proveedor de identidad. Por ejemplo, vRealize Automation 7.0 y versiones posteriores admiten vCenter Single Sign-On como un proveedor de identidad. Puede configurar una federación desde vCenter Single Sign-On y vRealize Automation. Después de esto, vCenter Single Sign-On puede realizar la autenticación cuando inicie sesión en vRealize Automation.

Para unir un proveedor de servicios SAML a la federación de identidades, tiene que configurar la confianza entre el SP y el IDP intercambiando los metadatos SAML entre ellos.

Debe realizar tareas de integración para vCenter Single Sign-On y el servicio que utiliza vCenter Single Sign-On.

1 Exporte los metadatos del IDP a un archivo y después impórtelos en el SP.

2 Exporte los metadatos del SP e impórtelos en el IDP.

Puede usar la interfaz de vSphere Web Client para vCenter Single Sign-On para exportar los metadatos del IDP y para importar los del SP. Si está usando vRealize Automation como el SP, consulte la documentación de vRealize Automation para obtener detalles sobre cómo exportar los metadatos del SP e importar los del IDP.

Nota El servicio debe admitir completamente el estándar SAML 2.0, de lo contrario, la integración no funcionará.

Unirse a un proveedor de servicios SAML a la federación de identidades

Puede usar vSphere Web Client para agregar un proveedor de servicios SAML a vCenter Single Sign-On y agregar vCenter Single Sign-On como el proveedor de identidad de ese servicio. Cuando los usuarios inicien sesión en el proveedor de servicios, este autenticará a los usuarios con vCenter Single Sign-On.

Requisitos previos

El servicio de destino debe ser totalmente compatible con el estándar SAML 2.0 y los metadatos del SP deben tener el elemento `SPSSODescriptor`.

Si los metadatos no siguen el esquema de metadatos de SAML 2.0 de forma precisa, puede que deba editar los metadatos antes de importarlos. Por ejemplo, si está utilizando un proveedor de servicios SAML de Servicios de federación de Active Directory (Active Directory Federation Services, ADFS), debe editar los metadatos para poder importarlos. Quite los siguientes elementos no estándar:

```
fed:ApplicationServiceType
fed:SecurityTokenServiceType
```

Procedimiento

1 Exporte los metadatos del proveedor de servicios a un archivo.

2 Inicie sesión con vSphere Web Client en la instancia de vCenter Server conectada a Platform Services Controller.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Importe los metadatos del SP a vCenter Single Sign-On.

   a Seleccione la pestaña **Proveedores de servicios SAML**.

   b En el cuadro de diálogo **Metadatos del proveedor de servicios SAML**, importe los metadatos pegando la cadena XML o importando un archivo.

5 Exporte los metadatos de IDP de vCenter Single Sign-On.

   a En el cuadro de texto **Metadatos para el proveedor de servicios SAML**, haga clic en **Descargar**.

   b Especifique una ubicación de archivo.

6 Inicie sesión en el SP de SAML, por ejemplo, VMware vRealize Automation 7.0, y siga las instrucciones del SP para agregar los metadatos de vCenter Single Sign-On a ese proveedor de servicios.

Consulte la documentación de vRealize Automation para obtener más detalles acerca de la importación de los metadatos en ese producto.

Servicio de token de seguridad (STS)

El servicio de token de seguridad (STS) de vCenter Single Sign-On es un servicio web que emite, valida y renueva los tokens de seguridad.

Los usuarios presentan sus credenciales principales a la interfaz de STS para adquirir tokens SAML. La credencial principal depende del tipo de usuario.

Usuario

Nombre de usuario y contraseña disponibles en un origen de identidad de vCenter Single Sign-On.

Usuario de la aplicación

Certificado válido.

El STS autentica al usuario en función de las credenciales principales y crea un token SAML que contiene los atributos del usuario. El STS firma el token SAML con su certificado de firma de STS y asigna el token al usuario. De forma predeterminada, VMCA genera el certificado de firma del STS. Puede reemplazar el certificado de firma predeterminado del STS desde vSphere Web Client. No reemplace el certificado de firma STS a menos que la directiva de seguridad de la empresa exija que se reemplacen todos los certificados.

Una vez que el usuario tiene un token SAML, este se envía como parte de las solicitudes HTTP del usuario, posiblemente a través de varios proxy. Únicamente el destinatario previsto (el proveedor de servicios) puede utilizar la información del token SAML.

Actualizar el certificado del servicio de token de seguridad

El servidor vCenter Single Sign-On incluye un servicio de token de seguridad (STS). El STS es un servicio web que emite, valida y renueva los tokens de seguridad. Puede actualizar manualmente el certificado actual del STS en vSphere Web Client cuando el certificado caduque o se modifique.

Para adquirir un token SAML, un usuario presenta las credenciales principales ante el STS. Las credenciales principales dependen del tipo de usuario:

Usuario de solución

Certificado válido

Otros usuarios

Nombre de usuario y contraseña disponibles en un origen de identidad de vCenter Single Sign-On.

El STS autentica al usuario mediante las credenciales principales y crea un token SAML que contiene los atributos del usuario. El servicio STS firma el token SAML con su certificado de firma de STS y, a continuación, asigna el token a un usuario. De forma predeterminada, VMCA genera el certificado de firma del STS.

Una vez que el usuario tiene un token SAML, este se envía como parte de las solicitudes HTTP del usuario, posiblemente a través de varios proxy. Únicamente el destinatario previsto (el proveedor de servicios) puede utilizar la información del token SAML.

Es posible reemplazar el certificado de firma de STS actual de vSphere Web Client si la directiva de la empresa así lo requiere o si se desea actualizar un certificado caducado.

Precaución No reemplace el archivo en el sistema de archivos. Si lo hace, se generarán errores inesperados y difíciles de depurar.

Nota Después de reemplazar el certificado, debe reiniciar el nodo para reiniciar los servicios STS y vSphere Web Client.

Requisitos previos

Copie el certificado que acaba de agregar al almacén de claves de Java desde Platform Services Controller en la estación de trabajo local.

Dispositivo de Platform Services Controller

`certificate_location/keys/root-trust.jks Por ejemplo: /keys/root-trust.jks`

Por ejemplo:

`/root/newsts/keys/root-trust.jks`

Instalación de Windows

`certificate_location\root-trust.jks`

Por ejemplo:

`C:\Archivos de programa\VMware\vCenter Server\jre\bin\root-trust.jks`

Procedimiento

1 Inicie sesión en vSphere Web Client como administrator@vsphere.local u otro usuario con privilegios de administrador de vCenter Single Sign-On.

   Los usuarios con privilegios de administrador de vCenter Single Sign-On están en el grupo Administradores, en el dominio de vCenter Single Sign-On local (de manera predeterminada, vsphere.local).

2 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

3 Seleccione la pestaña **Certificados**, la subpestaña **Firma de STS** y, a continuación, haga clic en el icono **Agregar certificado de firma de STS**.

4 Agregue el certificado.

   a Haga clic en **Examinar** para desplazarse hasta el archivo JKS de almacenamiento de claves que contiene el nuevo certificado y haga clic en **Abrir**.

   b Escriba la contraseña cuando se le solicite.

   c Haga clic en la parte superior de la cadena de alias de STS y haga clic en **Aceptar**.

   d Escriba la contraseña nuevamente cuando se le solicite.

5 Haga clic en **Aceptar**.

6 Reinicie el nodo de Platform Services Controller para iniciar tanto el servicio STS como vSphere Web Client.

   Antes de reiniciar, la autenticación no funciona correctamente, por lo que es esencial que reinicie.

Generar un nuevo certificado de firma de STS en el dispositivo

Como el certificado de firma del servicio de token de seguridad (Security Token Service, STS) de vCenter Single Sign-On es un certificado de VMware interno, no lo reemplace a menos que la empresa exija el reemplazo de los certificados internos. Si desea reemplazar el certificado de firma de STS predeterminado, debe generar un certificado nuevo y agregarlo al almacén de claves de Java. Este procedimiento explica los pasos en un dispositivo de implementación integrado o un dispositivo de Platform Services Controller externo.

Nota Este certificado es válido durante diez años y no es un certificado externo. No reemplace este certificado a menos que la directiva de seguridad de su empresa así lo exija.

Consulte Generar un nuevo certificado de firma de STS en una instalación de Windows de vCenter si está ejecutando una instalación de Windows de Platform Services Controller.

Procedimiento

1 Cree un directorio de nivel superior para mantener el nuevo certificado y compruebe la ubicación del directorio.

```
mkdir newsts
cd newsts
pwd
#resulting output: /root/newst
```

2 Copie el archivo `certool.cfg` en el nuevo directorio.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

3 Abra una copia del archivo `certool.cfg` y edítela para usar el nombre de host y la dirección IP de Platform Services Controller local.

El país es obligatorio y tiene que ser de dos caracteres, como se muestra en el siguiente ejemplo.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 Genere la clave.

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/
sts.key --pubkey=/root/newsts/sts.pub
```

5 Genere el certificado.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --privkey=/root/
newsts/sts.key --config=/root/newsts/certool.cfg
```

6 Convierta el certificado al formato PK12.

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key
-certfile /var/lib/vmware/vmca/root.cer -name "newstssigning" -passout pass:testpassword
-out newsts.p12
```

7 Agregue el certificado al almacén de claves de Java (Java Keystore, JKS).

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.p12 -srcstoretype
pkcs12 -srcstorepass testpassword -srcalias newstssigning -destkeystore root-trust.jks
-deststoretype JKS -deststorepass testpassword -destkeypass testpassword

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype
JKS -storepass testpassword -keypass testpassword -file /var/lib/vmware/vmca/root.cer
-alias root-ca
```

Utilice `keytool -help` para obtener una lista de todos los comandos disponibles.

8 Cuando se le solicite, escriba **Sí** para aceptar el certificado en el almacén de claves.

Pasos siguientes

Ahora puede importar el certificado nuevo. Consulte Actualizar el certificado del servicio de token de seguridad.

Generar un nuevo certificado de firma de STS en una instalación de Windows de vCenter

Como el certificado de firma del servicio de token de seguridad (Security Token Service, STS) de vCenter Single Sign-On es un certificado de VMware interno, no lo reemplace a menos que la empresa exija el reemplazo de los certificados internos. Si desea reemplazar el certificado de firma de STS predeterminado, primero debe generar un certificado nuevo y agregarlo al almacén de claves de Java. Este procedimiento explica los pasos en una instalación de Windows.

Nota Este certificado es válido durante diez años y no es un certificado externo. No reemplace este certificado a menos que la directiva de seguridad de su empresa así lo exija.

Consulte Generar un nuevo certificado de firma de STS en el dispositivo si está usando un dispositivo virtual.

Procedimiento

1 Cree un directorio para alojar el nuevo certificado.

```
cd C:\ProgramData\VMware\vCenterServer\cfg\sso\keys\
mkdir newsts
cd newsts
```

2 Realice una copia del archivo `certool.cfg` y colóquela en el nuevo directorio.

```
copy "C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg" .
```

3 Abra una copia del archivo `certool.cfg` y edítela para usar el nombre de host y la dirección IP de Platform Services Controller local.

El país es obligatorio y tiene que ser de dos caracteres. Esto se muestra en el siguiente ejemplo.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
```

```
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 Genere la clave.

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --server localhost --genkey --
privkey=sts.key --pubkey=sts.pub
```

5 Genere el certificado.

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --gencert --cert=newsts.cer --
privkey=sts.key --config=certool.cfg
```

6 Convierta el certificado al formato PK12.

```
"C:\Program Files\VMware\vCenter Server\openSSL\openssl.exe" pkcs12 -export -in newsts.cer
-inkey sts.key -certfile C:\ProgramData\VMware\vCenterServer\data\vmca\root.cer -name
"newstssigning" -passout pass:changeme -out newsts.p12
```

7 Agregue el certificado al almacén de claves de Java (Java Keystore, JKS).

```
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importkeystore
-srckeystore newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias
newstssigning -destkeystore root-trust.jks -deststoretype JKS -deststorepass testpassword
-destkeypass testpassword
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importcert -keystore
root-trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -file
C:\ProgramData\VMware\vCenterServer\data\vmca\root.cer -alias root-ca
```

Pasos siguientes

Ahora puede importar el certificado nuevo. Consulte Actualizar el certificado del servicio de token de seguridad.

Determinar la fecha de caducidad de un certificado SSL de LDAPS

Si selecciona un origen de identidad de LDAP y decide usar LDAPS, puede cargar un certificado SSL para el tráfico LDAP. Los certificados SSL caducan después de un tiempo predefinido. Si se conoce la fecha de caducidad de un certificado, se puede reemplazar o renovar el certificado antes de que caduque.

Solo puede ver la información de caducidad del certificado si utiliza un servidor LDAP u OpenLDAP de Active Directory, y si especifica una dirección URL `ldaps://` para el servidor. La pestaña **Almacén de confianza de orígenes de identidad** permanece vacía para los demás tipos de orígenes de identidad o para el tráfico de `ldap://`.

Procedimiento

1 Inicie sesión con vSphere Web Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en la pestaña **Orígenes de identidad**.

5 En la parte superior de la pantalla, seleccione el origen de identidad cuyo certificado LDAPS desee ver.

6 En la parte inferior de la pantalla, vea los detalles del certificado y compruebe la fecha de caducidad en el campo **Validar hasta**.

   Es posible que vea una advertencia en la parte superior de la pestaña que indica que un certificado está por caducar.

Administrar directivas de vCenter Single Sign-On

Las directivas de vCenter Single Sign-On aplican las reglas de seguridad en el entorno. Puede ver y editar la directiva de contraseñas, la directiva de bloqueo y la directiva de tokens de vCenter Single Sign-On predeterminadas.

Editar la directiva de contraseñas de vCenter Single Sign-On

La directiva de contraseñas de vCenter Single Sign-On determina el formato y la caducidad de la contraseña. La directiva de contraseñas se aplica solo a los usuarios del dominio de vCenter Single Sign-On (vsphere.local o vmc.local).

De forma predeterminada, las contraseñas de vCenter Single Sign-On caducan a los 90 días. vSphere Client recuerda al usuario cuando la contraseña está a punto de caducar.

Consulte Cambiar la contraseña de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Haga clic en **Directivas**, seleccione **Directiva de contraseñas** y haga clic en **Editar**.

5 Edite la directiva de contraseñas.

Opción	Descripción
Descripción	Descripción de directivas de contraseñas.
Duración máxima	Cantidad máxima de días de validez de la contraseña antes de que el usuario deba cambiarla. El número máximo de días que puede introducir es 999999999. Un valor de cero (0) significa que la contraseña nunca caduca.
Reutilización restringida	Cantidad de contraseñas anteriores que no pueden volver a utilizarse. Por ejemplo, si introduce 6, el usuario no puede volver a usar ninguna de las últimas seis contraseñas.
Longitud máxima	Cantidad máxima de caracteres que se permiten en la contraseña.
Longitud mínima	Cantidad mínima de caracteres que se requiere en la contraseña. La longitud mínima no debe ser inferior a la cantidad mínima requerida de caracteres alfabéticos, numéricos y especiales combinados.
Requisitos de caracteres	Cantidad mínima de tipos de caracteres diferentes que se requieren en la contraseña. Puede especificar la cantidad de caracteres de cada tipo de la siguiente manera: ■ Especiales: & # % ■ Alfabéticos: A b c D ■ Mayúsculas: A B C ■ Minúsculas: a b c ■ Numéricos: 1 2 3 La cantidad mínima de caracteres alfabéticos no debe ser inferior a la cantidad de caracteres en mayúscula y minúscula combinados. Se admiten caracteres no ASCII en las contraseñas. En versiones anteriores de vCenter Single Sign-On, hay limitaciones en los caracteres admitidos.
Caracteres adyacentes idénticos	Cantidad máxima de caracteres adyacentes idénticos que se permiten en la contraseña. Por ejemplo, si escribe 1, la siguiente contraseña no se permite: p@$$word. El número debe ser superior a 0.

6 Haga clic en **Guardar**.

Editar la directiva de bloqueo de vCenter Single Sign-On

Si un usuario intenta iniciar sesión con las credenciales equivocadas, una directiva de bloqueo de vCenter Single Sign-On especifica cuándo queda bloqueada la cuenta del usuario de vCenter Single Sign-On. Los administradores pueden editar la directiva de bloqueo.

Si un usuario inicia sesión varias veces en vsphere.local con la contraseña incorrecta, su cuenta se bloqueará. La directiva de bloqueo permite que los administradores especifiquen la cantidad máxima de intentos fallidos de inicio de sesión, y establezcan el intervalo entre un intento fallido y otro. En la directiva también se especifica cuánto tiempo debe transcurrir antes de que la cuenta se desbloquee automáticamente.

Nota La directiva de bloqueo se aplica únicamente a las cuentas de usuario, no a las cuentas de sistema, como administrator@vsphere.local.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Seleccione **Directiva de bloqueo** y haga clic en **Editar**.

5 Edite los parámetros.

Opción	Descripción
Descripción	Descripción opcional de la directiva de bloqueo.
Cantidad máxima de intentos fallidos de inicio de sesión	Cantidad máxima de intentos fallidos de inicio de sesión permitidos antes de que la cuenta se bloquee.
Intervalo entre intentos fallidos	Período en el cual deben ocurrir los intentos fallidos de inicio de sesión para activar un bloqueo.
Tiempo de desbloqueo	Cantidad de tiempo durante la cual permanece bloqueada la cuenta. Si introduce 0, el administrador debe desbloquear la cuenta explícitamente.

6 Haga clic en **Guardar**.

Editar la directiva de tokens de vCenter Single Sign-On

La directiva de tokens de vCenter Single Sign-On especifica las propiedades de tokens, como la tolerancia de reloj y el recuento de renovaciones. Puede editar la directiva de tokens para que la especificación de los tokens se adapte a los estándares de seguridad de la empresa.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign On**, haga clic en **Configuración**.

4 Seleccione **Directiva de tokens** y haga clic en **Editar**.

5 Edite los parámetros de configuración de la directiva de tokens.

Opción	Descripción
Tolerancia de reloj	Diferencia horaria, en milisegundos, que vCenter Single Sign-On tolera entre un reloj de cliente y el reloj de la controladora de dominio. Si la diferencia horaria es mayor que el valor especificado, vCenter Single Sign-On declara al token como no válido.
Recuento máximo de renovaciones de token	Es la máxima cantidad de veces que puede renovarse un token. Una vez alcanzada la cantidad máxima de intentos de renovación, se requiere un nuevo token de seguridad.
Recuento máximo de delegaciones de token	Los tokens HoK (Holder-of-key) pueden delegarse a servicios del entorno vSphere. Un servicio que emplea un token delegado ejecuta dicho servicio en nombre del servicio principal que proporcionó el token. La solicitud de un token especifica una identidad DelegateTo. El valor de DelegateTo puede ser el token de una solución o una referencia al token de la solución. Este valor especifica cuántas veces puede delegarse un mismo token HoK.
Duración máxima de token de portador	Los tokens de portador proporcionan autenticación basada únicamente en la posesión del token. Los tokens de portador están pensados para el uso a corto plazo y para una única operación. El token de portador no comprueba la identidad del usuario o de la entidad que envía la solicitud. Este valor especifica la duración del token de portador antes de que el token deba emitirse nuevamente.
Duración máxima de token HoK	Los tokens HoK proporcionan autenticación basada en los artefactos de seguridad que están integrados en el token. Los tokens HoK pueden usarse para operaciones de delegación. Un cliente puede obtener un token HoK y delegarlo a otra entidad. El token contiene las notificaciones para identificar al originador y al delegado. En el entorno vSphere, un sistema vCenter Server obtiene tokens delegados en nombre de un usuario y los utiliza para realizar operaciones. Este valor determina la duración de un token HoK antes de que el token se marque como no válido.

6 Haga clic en **Guardar**.

Editar la notificación de caducidad de la contraseña para usuarios de Active Directory

La notificación de caducidad de la contraseña de Active Directory se realiza de manera independiente de la caducidad de la contraseña de vCenter Server SSO. De forma

predeterminada, la notificación de caducidad de la contraseña para un usuario de Active Directory se envía tras 30 días, pero la fecha de caducidad real de la contraseña depende del sistema de Active Directory. vSphere Client y vSphere Web Client controlan la notificación de caducidad. Puede cambiar la notificación de caducidad predeterminada para cumplir con los estándares de seguridad de su empresa.

Procedimiento

1 Inicie sesión en el sistema vCenter Server como usuario con privilegios de administrador.

   El usuario predeterminado con la función de superadministrador es root.

2 Cambie el directorio a la ubicación del archivo `webclient.properties`.

Sistema operativo	Comando
Linux	■ vSphere Client: `cd /etc/vmware/vsphere-ui` ■ vSphere Web Client: `cd /etc/vmware/vsphere-client`
Windows	■ vSphere Client: `cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-ui` ■ vSphere Web Client: `cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-client`

3 Abra el archivo `webclient.properties` con un editor de texto.

4 Edite la siguiente variable.

```
sso.pending.password.expiration.notification.days = 30
```

5 Reinicie el cliente.

Sistema operativo	Comando
Linux	■ vSphere Client: `service-control --stop vsphere-ui` `service-control --start vsphere-ui` ■ vSphere Web Client: `service-control --stop vsphere-client` `service-control --start vsphere-client`
Windows	■ vSphere Client: `cd "C:\Program Files\VMware\vCenter Server\bin\"` `service-control --stop vsphere-ui` `service-control --start vsphere-ui` ■ vSphere Web Client: `cd "C:\Program Files\VMware\vCenter Server\bin\"` `service-control --stop vspherewebclientsvc` `service-control --start vspherewebclientsvc`

Administrar usuarios y grupos de vCenter Single Sign-On

Un usuario administrador de vCenter Single Sign-On puede administrar usuarios y grupos en el dominio vsphere.local desde vSphere Client.

El usuario administrador de vCenter Single Sign-On puede realizar las siguientes tareas.

- Agregar usuarios de vCenter Single Sign-On

  Los usuarios que aparecen en la pestaña **Usuarios** en vSphere Client son internos de vCenter Single Sign-On y pertenecen al dominio vsphere.local. Puede agregar usuarios a ese dominio en una de las interfaces de administración de vCenter Single Sign-On.

- Deshabilitar y habilitar usuarios de vCenter Single Sign-On

  Cuando se deshabilita una cuenta de usuario de vCenter Single Sign-On, el usuario no puede iniciar sesión en el servidor de vCenter Single Sign-On hasta que un administrador habilite la cuenta. Es posible habilitar y deshabilitar cuentas desde una de las interfaces de administración de vCenter Single Sign-On.

- Eliminar un usuario de vCenter Single Sign-On

  Puede eliminar usuarios que se encuentran en el dominio vsphere.local desde una interfaz de administración de vCenter Single Sign-On. No puede eliminar usuarios del sistema operativo local ni usuarios de otro dominio desde una interfaz de administración de vCenter Single Sign-On.

- Editar un usuario de vCenter Single Sign-On

  Puede cambiar la contraseña u otros detalles de un usuario de vCenter Single Sign-On desde una interfaz de administración de vCenter Single Sign-On. No puede cambiar el nombre de los usuarios en el dominio vsphere.local. Esto significa que no puede cambiar el nombre de administrator@vsphere.local.

- Agregar un grupo de vCenter Single Sign-On

  La pestaña **Grupos** de vCenter Single Sign-On muestra los grupos del dominio local (de manera predeterminada, vsphere.local). Puede agregar grupos si necesita un contenedor para miembros de grupos (entidades de seguridad).

- Agregar miembros a un grupo de vCenter Single Sign-On

  Los miembros de un grupo de vCenter Single Sign-On pueden ser usuarios u otros grupos de uno o más orígenes de identidad. Puede agregar miembros nuevos de vSphere Client.

- Quitar miembros de un grupo de vCenter Single Sign-On

  Es posible eliminar miembros de un grupo de vCenter Single Sign-On mediante vSphere Client. Al quitar un miembro (usuario o grupo) de un grupo local, el miembro no se elimina del sistema.

- Eliminar usuarios de solución vCenter Single Sign-On

  vCenter Single Sign-On muestra a los usuarios de solución. Un usuario de solución es una recopilación de servicios. Como parte de la instalación, se definen de forma previa varios usuarios de solución vCenter Server que se autentican en vCenter Single Sign-On. En situaciones de solución de problemas, por ejemplo, si no se completó correctamente una desinstalación, es posible eliminar usuarios individuales de la solución desde vSphere Web Client.

- Cambiar la contraseña de vCenter Single Sign-On

  Los usuarios del dominio local, vsphere.local de forma predeterminada, pueden cambiar las contraseñas de vCenter Single Sign-On desde una interfaz web. Los usuarios de otros dominios pueden cambiar la contraseña mediante las reglas de ese dominio.

Agregar usuarios de vCenter Single Sign-On

Los usuarios que aparecen en la pestaña **Usuarios** en vSphere Client son internos de vCenter Single Sign-On y pertenecen al dominio vsphere.local. Puede agregar usuarios a ese dominio en una de las interfaces de administración de vCenter Single Sign-On.

Puede seleccionar otros dominios y ver en ellos información sobre los usuarios, pero no puede agregar usuarios a otros dominios desde una interfaz de administración de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Si el dominio actualmente seleccionado no es vsphere.local, selecciónelo en el menú desplegable.

   No puede agregar usuarios a otros dominios.

5 En la pestaña **Usuarios**, haga clic en **Agregar usuario**.

6 Escriba un nombre de usuario y una contraseña para el nuevo usuario.

   No puede cambiar el nombre de usuario una vez creado el usuario. La contraseña debe cumplir con los requisitos de la directiva de contraseñas del sistema.

7 (opcional) Escriba el nombre y el apellido del nuevo usuario.

8 (opcional) Introduzca una dirección de correo electrónico y una descripción del usuario.

9 Haga clic en **Agregar**.

Resultados

Cuando agrega un usuario, este en principio no tiene privilegios para realizar operaciones de administración.

Pasos siguientes

Agregue el usuario a un grupo del dominio vsphere.local, por ejemplo, al grupo de usuarios que pueden administrar VMCA (Administradores de CA) o al grupo de usuarios que pueden administrar vCenter Single Sign-On (Administradores). Consulte Agregar miembros a un grupo de vCenter Single Sign-On.

Deshabilitar y habilitar usuarios de vCenter Single Sign-On

Cuando se deshabilita una cuenta de usuario de vCenter Single Sign-On, el usuario no puede iniciar sesión en el servidor de vCenter Single Sign-On hasta que un administrador habilite la cuenta. Es posible habilitar y deshabilitar cuentas desde una de las interfaces de administración de vCenter Single Sign-On.

Las cuentas de usuario deshabilitadas permanecen disponibles en el sistema vCenter Single Sign-On, pero el usuario no puede iniciar sesión ni realizar operaciones en el servidor. Los usuarios con privilegios de administrador pueden deshabilitar y habilitar cuentas desde la página **Usuarios y grupos** de vCenter.

Requisitos previos

Debe ser miembro del grupo de administradores de vCenter Single Sign-On para deshabilitar y habilitar usuarios de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Seleccione un nombre de usuario, haga clic en el icono de tres puntos verticales y, luego, en **Deshabilitar**.

5 Haga clic en **Aceptar**.

6 Para volver a habilitar al usuario, haga clic en el icono de tres puntos verticales, haga clic en **Habilitar** y, luego, en **Aceptar**.

Eliminar un usuario de vCenter Single Sign-On

Puede eliminar usuarios que se encuentran en el dominio vsphere.local desde una interfaz de administración de vCenter Single Sign-On. No puede eliminar usuarios del sistema operativo local ni usuarios de otro dominio desde una interfaz de administración de vCenter Single Sign-On.

Precaución Si elimina el usuario administrador del dominio vsphere.local, ya no podrá iniciar sesión en vCenter Single Sign-On. Reinstale vCenter Server y sus componentes.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Seleccione **Usuarios** y el dominio vsphere.local en el menú desplegable.

5 En la lista de usuarios, seleccione el usuario que desea eliminar y haga clic en el icono de tres puntos verticales.

6 Haga clic en **Eliminar**.

   Proceda con precaución, ya que esta acción no se puede deshacer.

Editar un usuario de vCenter Single Sign-On

Puede cambiar la contraseña u otros detalles de un usuario de vCenter Single Sign-On desde una interfaz de administración de vCenter Single Sign-On. No puede cambiar el nombre de los usuarios en el dominio vsphere.local. Esto significa que no puede cambiar el nombre de administrator@vsphere.local.

Puede crear usuarios adicionales con los mismos privilegios de administrator@vsphere.local.

Los usuarios de vCenter Single Sign-On se almacenan en el dominio vsphere.local de vCenter Single Sign-On.

Puede revisar las directivas sobre contraseñas de vCenter Single Sign-On desde vSphere Client. Inicie sesión como administrator@vsphere.local y en el menú **Administración**, seleccione **Configuración > Directivas > Directiva de contraseñas**.

Consulte también Editar la directiva de contraseñas de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Haga clic en **Usuarios**.

5 Haga clic en el icono de tres puntos verticales y seleccione **Editar**.

6 Edite los atributos del usuario.

   No puede cambiar el nombre de usuario.

   La contraseña debe cumplir con los requisitos de la directiva de contraseñas del sistema.

7 Haga clic en **Aceptar**.

Agregar un grupo de vCenter Single Sign-On

La pestaña **Grupos** de vCenter Single Sign-On muestra los grupos del dominio local (de manera predeterminada, vsphere.local). Puede agregar grupos si necesita un contenedor para miembros de grupos (entidades de seguridad).

No puede agregar grupos a otros dominios (por ejemplo, el dominio de Active Directory) desde la pestaña **Grupos** de vCenter Single Sign-On.

Si no agrega un origen de identidad a vCenter Single Sign-On, la creación de grupos y la incorporación de usuarios pueden ayudarlo a organizar el dominio local.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Seleccione **Grupos** y haga clic en **Agregar grupo**.

5 Introduzca un nombre y una descripción para el grupo.

   No puede cambiar el nombre de grupo una vez creado el grupo.

6 Haga clic en **Agregar**.

Pasos siguientes

- Agregue miembros al grupo.

Agregar miembros a un grupo de vCenter Single Sign-On

Los miembros de un grupo de vCenter Single Sign-On pueden ser usuarios u otros grupos de uno o más orígenes de identidad. Puede agregar miembros nuevos de vSphere Client.

Consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2095342 para obtener información de fondo.

Los grupos que se enumeran en la pestaña **Grupos** de la interfaz web son parte del dominio vsphere.local. Consulte Grupos del dominio de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Haga clic en la pestaña **Grupos** y, a continuación, en el grupo (por ejemplo, Administradores).

5 En el área Miembros de grupo, haga clic en el icono **Agregar miembros**.

6 Seleccione el origen de identidad que contenga el miembro que se va a agregar al grupo.

7 (opcional) Introduzca un término de búsqueda y haga clic en **Buscar**.

8 Seleccione al miembro.

   Puede agregar más de un miembro.

9 Haga clic en **Aceptar**.

Quitar miembros de un grupo de vCenter Single Sign-On

Es posible eliminar miembros de un grupo de vCenter Single Sign-On mediante vSphere Client. Al quitar un miembro (usuario o grupo) de un grupo local, el miembro no se elimina del sistema.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Seleccione los **Grupos** y haga clic en un grupo.

5 En la lista de miembros del grupo, seleccione el usuario o el grupo que desea eliminar y, a continuación, haga clic en el icono de tres puntos verticales.

6 Haga clic en **Quitar miembro**.

7 Haga clic en **Quitar**.

Resultados

El usuario se elimina del grupo, pero sigue disponible en el sistema.

Eliminar usuarios de solución vCenter Single Sign-On

vCenter Single Sign-On muestra a los usuarios de solución. Un usuario de solución es una recopilación de servicios. Como parte de la instalación, se definen de forma previa varios usuarios de solución vCenter Server que se autentican en vCenter Single Sign-On. En situaciones de solución de problemas, por ejemplo, si no se completó correctamente una desinstalación, es posible eliminar usuarios individuales de la solución desde vSphere Web Client.

Cuando se elimina el conjunto de servicios asociados con un usuario de solución vCenter Server o un usuario de una solución externa desde el entorno, el usuario de solución se elimina de la pantalla de vSphere Web Client. Si se elimina una aplicación de manera forzosa, o si no se puede recuperar el sistema mientras el usuario de solución sigue en el sistema, es posible eliminar el usuario de solución explícitamente desde vSphere Web Client.

Importante Si se elimina un usuario de solución, los servicios correspondientes ya no se pueden autenticar en vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Web Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de configuración de usuario de vCenter Single Sign-On.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Single Sign-On**, haga clic en **Usuarios y grupos**.

4 Haga clic en la pestaña **Usuarios de la solución** y seleccione el nombre de un usuario de solución.

5 Haga clic en el icono **Eliminar usuario de solución**.

6 Haga clic en **Sí**.

Resultados

Los servicios asociados con el usuario de solución ya no tendrán acceso a vCenter Server y no podrán funcionar como servicios de vCenter Server.

Cambiar la contraseña de vCenter Single Sign-On

Los usuarios del dominio local, vsphere.local de forma predeterminada, pueden cambiar las contraseñas de vCenter Single Sign-On desde una interfaz web. Los usuarios de otros dominios pueden cambiar la contraseña mediante las reglas de ese dominio.

La directiva de bloqueo de vCenter Single Sign-On determina el momento en que caduca la contraseña. De forma predeterminada, las contraseñas de usuario de vCenter Single Sign-On caducan a los 90 días, pero las contraseñas de administrador, como la de administrator@vsphere.local, no caducan. Las interfaces de administración de vCenter Single Sign-On muestran una advertencia cuando la contraseña está por caducar.

Nota Solo puede cambiar una contraseña si no ha caducado.

Si la contraseña ha caducado, el administrador del dominio local, administrator@vsphere.local de forma predeterminada, puede restablecerla mediante el comando `dir-cli password reset`. Solo pueden restablecer contraseñas los miembros del grupo Administrador para el dominio de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 En el panel de navegación superior, a la derecha del menú Ayuda, haga clic en su nombre de usuario para desplegar el menú.

   Otra opción es seleccionar **Single Sign-On > Usuarios y grupos** y, a continuación, seleccionar **Editar usuario** en el menú de tres puntos verticales.

4 Seleccione **Cambiar contraseña** y escriba la contraseña actual.

5 Escriba la nueva contraseña y confírmela.

   La contraseña debe cumplir con la directiva de contraseñas.

6 Haga clic en **Aceptar**.

Prácticas recomendadas de seguridad de vCenter Single Sign-On

Siga las prácticas recomendadas de seguridad de vCenter Single Sign-On para proteger el entorno de vSphere.

La infraestructura de autenticación de vSphere optimiza la seguridad del entorno de vSphere. Para garantizar que la infraestructura no se vea comprometida, siga las prácticas recomendadas de vCenter Single Sign-On.

Compruebe la caducidad de las contraseñas

La directiva predeterminada de contraseñas de vCenter Single Sign-On establece una duración de 90 días para las contraseñas. Después de 90 días, la contraseña caduca y ya no puede iniciar sesión. Compruebe la fecha de caducidad y actualice las contraseñas oportunamente.

Configure NTP

Compruebe que todos los sistemas tengan el mismo origen de hora relativo (incluida la correspondiente compensación por localización), y que este pueda ser correlativo con una hora estándar acordada (como la hora universal coordenada, UTC). La sincronización de los sistemas es fundamental para la validez de los certificados de vCenter Single Sign-On y de otros certificados de vSphere.

NTP también facilita el rastreo de intrusos en los archivos de registro. Una configuración incorrecta de la hora puede dificultar la inspección y la correlación de los archivos de registro a fin de detectar ataques; también puede hacer imprecisas las auditorías.

Certificados de seguridad de vSphere

3

vSphere proporciona seguridad mediante el uso de certificados para cifrar las comunicaciones, autenticar los servicios y firmar tokens.

vSphere utiliza certificados para:

- Cifrar las comunicaciones entre dos nodos, por ejemplo, vCenter Server y un host de ESXi.
- Autenticar los servicios de vSphere.
- Realizar acciones internas, como firmar tokens.

La entidad de certificación interna de vSphere, VMware Certificate Authority (VMCA) proporciona todos los certificados necesarios para vCenter Server y ESXi. VMCA se instala en cada Platform Services Controller y protege inmediatamente la solución sin realizar otras modificaciones. Mantener esta configuración predeterminada proporciona la sobrecarga operativa más baja para la administración de certificados. vSphere proporciona un mecanismo para renovar estos certificados en caso de que caduquen.

vSphere también proporciona un mecanismo para reemplazar determinados certificados con sus propios certificados. Sin embargo, reemplace solamente el certificado SSL que proporciona cifrado entre los nodos, para reducir la sobrecarga de administración de certificados al mínimo.

Se recomiendan las siguientes opciones para la administración de certificados.

Tabla 3-1. Opciones recomendadas para la administración de certificados

Modo	Descripción	Ventajas
Certificados de VMCA predeterminados	VMCA proporciona todos los certificados para hosts de vCenter Server y de ESXi.	Sobrecarga más simple y más baja. VMCA puede administrar el ciclo de vida de certificados para vCenter Server y hosts ESXi.
Certificados de VMCA predeterminados con certificados SSL externos (modo híbrido)	Para administrar certificados de los usuarios de solución y los hosts ESXi, debe reemplazar los certificados SSL de Platform Services Controller y vCenter Server Appliance, y permitir VMCA. De manera opcional, para las implementaciones de alta seguridad conscientes, puede reemplazar también los certificados SSL de host ESXi.	Simple y seguro. VMCA administra los certificados internos, pero se obtiene el beneficio de obtener sus certificados SSL aprobados por la empresa y que los exploradores confíen en dichos certificados.

VMware no recomienda el reemplazo de los certificados de usuario de la solución o los certificados STS ni el uso de una entidad de certificación subordinada en lugar de VMCA. Si selecciona cualquiera de estas opciones, es posible que se encuentre con una considerable complejidad y que exista la posibilidad de un impacto negativo para la seguridad y un aumento innecesario en el riesgo operativo. Para obtener más información sobre la administración de certificados en un entorno de vSphere, consulte la publicación de blog llamada *Revisión de producto nuevo: reemplazo del certificado SSL de vSphere híbrido* en http://vmware.com/go/hybridvmca.

Puede utilizar las siguientes opciones para reemplazar los certificados existentes:

Tabla 3-2. Diferentes enfoques de reemplazo de certificados

Opción	Consulte
Utilice vSphere Client. A partir de vSphere 6.7, Platform Services Controller se administra a través de vSphere Client.	Administrar certificados con vSphere Client
Ejecute la utilidad vSphere Certificate Manager desde la línea de comandos.	Administrar certificados con la utilidad vSphere Certificate Manager
Utilice los comandos de la CLI para el reemplazo manual de certificados.	Capítulo 4 Administrar servicios y certificados con comandos de CLI



Administración de certificados de vSphere (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ejp3dqkt/uiConfId/49694343/)

Este capítulo incluye los siguientes temas:

- Requisitos de certificados para distintas rutas de acceso de la solución
- Descripción general de la administración de certificados
- Administrar certificados con vSphere Client

- Administrar certificados desde vSphere Web Client
- Administrar certificados con la utilidad vSphere Certificate Manager
- Reemplazar certificados de forma manual

Requisitos de certificados para distintas rutas de acceso de la solución

Los requisitos de certificados dependen de si se usa VMCA como entidad de certificación intermedia o si se usan certificados personalizados. Los requisitos también son diferentes para los certificados de máquina y los certificados de usuario de solución.

Antes de comenzar, asegúrese de que la hora de todos los nodos del entorno esté sincronizada.

Requisitos para todos los certificados importados

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- SubjectAltName debe contener DNS Name=*machine_FQDN*
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, cifrado de clave.
- El uso mejorado de clave puede estar vacío o contener autenticación del servidor.

vSphere no admite los siguientes certificados.

- Certificados con comodines.
- No se recomiendan los algoritmos md2WithRSAEncryption 1.2.840.113549.1.1.2, md5WithRSAEncryption 1.2.840.113549.1.1.4 ni sha1WithRSAEncryption 1.2.840.113549.1.1.5.
- El algoritmo RSASSA-PSS con el OID 1.2.840.113549.1.1.10 no es compatible.

Cumplimiento del certificado con RFC 2253

El certificado debe cumplir con RFC 2253.

Si no genera solicitudes de firma de certificados (Certificate Signature Request, CSR) con Certificate Manager, asegúrese de que la CSR incluya los siguientes campos.

Cadena	Tipo de atributo X.500
CN	`commonName`
L	`localityName`
ST	`stateOrProvinceName`
O	`organizationName`

Cadena	Tipo de atributo X.500
OU	`organizationalUnitName`
C	`countryName`
CALLE	`streetAddress`
DC	`domainComponent`
UID	`userid`

Si genera CSR mediante Certificate Manager, se le pedirá la siguiente información y Certificate Manager agregará los campos correspondientes al archivo de CSR.

- La contraseña del usuario administrator@vsphere.local o del administrador del dominio de vCenter Single Sign-On al que se va a conectar.
- Cuando se desea generar una CSR en un entorno con una instancia externa de Platform Services Controller, se solicita el nombre de host o la dirección IP de Platform Services Controller.
- Información que Certificate Manager almacena en el archivo `certool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.
  - Contraseña de administrator@vsphere.local.
  - Código de país de dos letras
  - Nombre de empresa
  - Nombre de organización
  - Unidad de organización
  - Estado
  - Localidad
  - Dirección IP (opcional)
  - Correo electrónico
  - Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
  - Dirección IP de Platform Services Controller si se ejecuta el comando en un nodo de vCenter Server (administración).

Requisitos al usar VMCA como entidad de certificación intermedia

Cuando se utiliza VMCA como entidad de certificación intermedia, los certificados deben cumplir los siguientes requisitos.

Tipo de certificado	Requisitos de certificados
Certificado raíz	■ Se puede utilizar vSphere Certificate Manager para crear la CSR. Consulte Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia). ■ Si prefiere crear la CSR de forma manual, el certificado que envíe para firmar debe cumplir con los siguientes requisitos. ■ Tamaño de clave: 2.048 bits o más ■ Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8. ■ x509 versión 3 ■ Si utiliza certificados personalizados, la extensión CA debe establecerse con el valor true para certificados de raíz, y el signo cert debe estar en la lista de requisitos. ■ La firma CRL debe estar habilitada. ■ El uso mejorado de clave puede estar vacío o contener autenticación del servidor. ■ No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados. ■ No se admiten los certificados con comodines o con más de un nombre DNS. ■ No se pueden crear CA subsidiarias de VMCA. Para obtener un ejemplo de uso de la entidad de certificación de Microsoft, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2112009, Crear una plantilla de entidad de certificación de Microsoft para creación de certificados SSL en vSphere 6.0.
Certificado SSL de máquina	Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR. Si crea manualmente la CSR, debe cumplir con los requisitos enumerados anteriormente en la sección *Requisitos para todos los certificados importados*. También tendrá que especificar el FQDN del host.
Certificado de usuario de solución	Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR. **Nota** Debe utilizar un valor diferente en el nombre para cada usuario de solución. Si genera el certificado manualmente, es posible que esto se muestre como **CN** en el **asunto**, según la herramienta que utilice.

Tipo de certificado	Requisitos de certificados
	Si utiliza vSphere Certificate Manager, la herramienta le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en `certool.cfg`. Consulte la *información que solicita Certificate Manager*.

Requisitos de certificados personalizados

Si desea utilizar certificados personalizados, los certificados deben cumplir los siguientes requisitos.

Tipo de certificado	Requisitos de certificados
Certificado SSL de máquina	El certificado SSL de máquina en cada nodo debe tener un certificado independiente de la entidad de certificación empresarial o externa. - Puede generar la CSR mediante vSphere Client o vSphere Certificate Manager, o bien puede crearla de forma manual. La CSR debe cumplir con los requisitos enumerados anteriormente en la sección *Requisitos para todos los certificados importados*. - Si utiliza vSphere Certificate Manager, la herramienta le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en `certool.cfg`. Consulte la *información que solicita Certificate Manager*. - En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.
Certificado de usuario de solución	Cada usuario de solución en cada nodo debe tener un certificado independiente de la entidad de certificación empresarial o externa. - Puede generar la CSR mediante vSphere Certificate Manager o prepararla usted mismo. La CSR debe cumplir con los requisitos enumerados anteriormente en la sección *Requisitos para todos los certificados importados*. - Si utiliza vSphere Certificate Manager, la herramienta le solicitará información del certificado para cada usuario de solución. vSphere Certificate Manager almacena la información en `certool.cfg`. Consulte la *información que solicita Certificate Manager*. **Nota** Debe utilizar un valor diferente en el nombre para cada usuario de solución. Un certificado generado manualmente se puede mostrar como **CN** en el **asunto**, según la herramienta que utilice. Cuando reemplace posteriormente los certificados de usuario de solución por certificados personalizados, proporcione la cadena de certificados de firma completa de la entidad de certificación externa.

Nota No utilice los puntos de distribución de CRL, el acceso a la información de autoridad o la información de la plantilla de certificado en ningún certificado personalizado.

Descripción general de la administración de certificados

El trabajo requerido para configurar o actualizar la infraestructura de certificados depende de los requisitos de su entorno. Debe tener en cuenta si se está realizando una instalación nueva o una actualización, y si se está considerando ESXi o vCenter Server.

Administradores que no reemplazan certificados de VMware

VMCA puede encargarse de toda la administración de certificados. VMCA aprovisiona a vCenter Server con componentes y hosts ESXi con certificados que usan VMCA como entidad de certificación raíz. Si está actualizando a vSphere 6 desde una versión anterior de vSphere, todos los certificados autofirmados se reemplazan con certificados firmados por VMCA.

Si actualmente no reemplaza certificados de VMware, el entorno comienza a usar certificados firmados por VMCA en lugar de certificados autofirmados.

Administradores que reemplazan certificados de VMware por certificados personalizados

Si la directiva de la empresa exige certificados firmados por una CA de terceros o empresarial, o que requieran información de certificados personalizados, existen varias opciones para una instalación nueva.

- Que el certificado raíz de VMCA sea firmado por una CA independiente o una CA empresarial. Reemplazar el certificado raíz de VMCA con ese certificado firmado. En este escenario, el certificado de VMCA es un certificado intermedio. VMCA aprovisiona a los componentes de vCenter Server y a los hosts ESXi con certificados que incluyen la cadena completa de certificados.
- Si la directiva de la empresa no permite certificados intermedios en la cadena, los certificados se pueden reemplazar de manera explícita. Puede usar la utilidad vSphere Client, vSphere Certificate Manager o realizar el reemplazo manual de los certificados mediante la CLI de administración de certificados.

Cuando actualice un entorno que usa certificados personalizados, puede retener algunos.

- Los hosts ESXi mantienen sus certificados personalizados durante la actualización. Asegúrese de que el proceso de actualización de vCenter Server agregue todos los certificados raíz relevantes al almacén TRUSTED_ROOTS en VECS en vCenter Server.

  Después de la actualización a vSphere 6.0 o posteriores, se puede establecer el modo de certificado en **Personalizado**. Si el modo de certificación es el predeterminado (VMCA) y el usuario actualiza el certificado desde vSphere Client, los certificados firmados por VMCA reemplazan a los certificados personalizados.
- En el caso de los componentes de vCenter Server, lo que suceda dependerá del entorno actual.
  - En una actualización de una instalación simple a una implementación integrada, vCenter Server retiene los certificados personalizados. Después de la actualización, el entorno funcionará como antes.
  - Para una actualización de una implementación de varios sitios, vCenter Single Sign-On puede estar en un equipo diferente que otros componentes de vCenter Server. En ese caso, el proceso de actualización crea una implementación de varios nodos que incluye un nodo de Platform Services Controller y uno o varios nodos de administración.

Este escenario retiene los certificados de vCenter Server y vCenter Single Sign-On existentes. Los certificados se usan como certificados SSL de equipos.

Además, VMCA asigna un certificado firmado por VMCA a cada usuario de solución (recopilación de servicios de vCenter). El usuario de solución utiliza este certificado solo para autenticarse ante vCenter Single Sign-On. Con frecuencia, una directiva de la empresa no requiere el reemplazo de los certificados de usuarios de solución.

Ya no podrá usar la herramienta de reemplazo de certificados de vSphere 5.5, que estaba disponible para las instalaciones de vSphere 5.5. La nueva arquitectura resulta en una selección y distribución diferentes de los servicios. Una nueva utilidad de la línea de comandos, vSphere Certificate Manager, está disponible para la mayoría de las tareas de administración de certificados.

Interfaces de certificados de vSphere

En el caso de vCenter Server, es posible ver y reemplazar certificados con las siguientes herramientas e interfaces.

Tabla 3-3. Interfaces para administrar certificados de vCenter Server

Interfaz	Uso
vSphere Client	Realice tareas de certificados comunes con una interfaz gráfica de usuario.
Utilidad vSphere Certificate Manager	Realice tareas de reemplazo de certificados comunes desde la línea de comandos de la instalación de vCenter Server.
CLI de administración de certificados	Realice todas las tareas de administración de certificados con `dir-cli`, `certool` y `vecs-cli`.
vSphere Web Client	Vea los certificados, incluida la información de caducidad.

En el caso de ESXi, puede realizar la administración de certificados desde vSphere Client. VMCA aprovisiona certificados y los almacena localmente en el host ESXi. VMCA no almacena certificados de hosts ESXi en VMDIR o en VECS. Consulte la documentación de *Seguridad de vSphere*.

Certificados de vCenter admitidos

En el caso de vCenter Server, Platform Services Controller, y las máquinas y los servicios relacionados, se admiten los siguientes certificados:

- Certificados generados y firmados por la entidad de certificación VMware Certificate Authority (VMCA).
- Certificados personalizados.
  - Certificados empresariales que se generan desde su propia PKI interna.
  - Certificados externos firmados por una entidad de certificación que se genera mediante una PKI externa como Verisign, GoDaddy, etc.

No se admiten los certificados autofirmados que se crearon mediante OpenSSL donde no existe una entidad de certificación raíz.

Descripción general del reemplazo de certificados

Es posible realizar distintos tipos de reemplazo de certificados según los requisitos y la directiva de la empresa para el sistema que va a configurar. Se pueden reemplazar certificados desde Platform Services Controller con la utilidad vSphere Certificate Manager o manualmente mediante las CLI que se incluyen con la instalación.

VMCA se incluye en cada Platform Services Controller y en cada implementación integrada. VMCA aprovisiona cada nodo, cada usuario de la solución vCenter Server y cada host ESXi con un certificado firmado por VMCA en su calidad de entidad de certificación. Los usuarios de la solución vCenter Server son grupos de servicios de vCenter Server.

Es posible reemplazar los certificados predeterminados. Para los componentes de vCenter Server, puede usar un conjunto de herramientas de línea de comandos que se incluyen en la instalación. Existen varias opciones.

Reemplazar los certificados firmados por la VMCA

Si su certificado de VMCA vence o si quiere reemplazarlo por otros motivos, puede usar las CLI de administración de certificados para realizar ese proceso. De forma predeterminada, el certificado raíz de VMCA vence después de 10 años y todos los certificados que firma la VMCA vencen cuando caduca el certificado raíz, es decir, después de un máximo de 10 años.

Figura 3-1. Los certificados firmados por VMCA se almacenan en VECS

VMCA
Certificado de CA
Firmado
Certificado de máquina
VECS

Puede usar las siguientes opciones de vSphere Certificate Manager:

- Reemplazar un certificado de SSL de una máquina con un certificado de VMCA
- Reemplazo de un certificado de un usuario de una solución con un certificado de VMCA

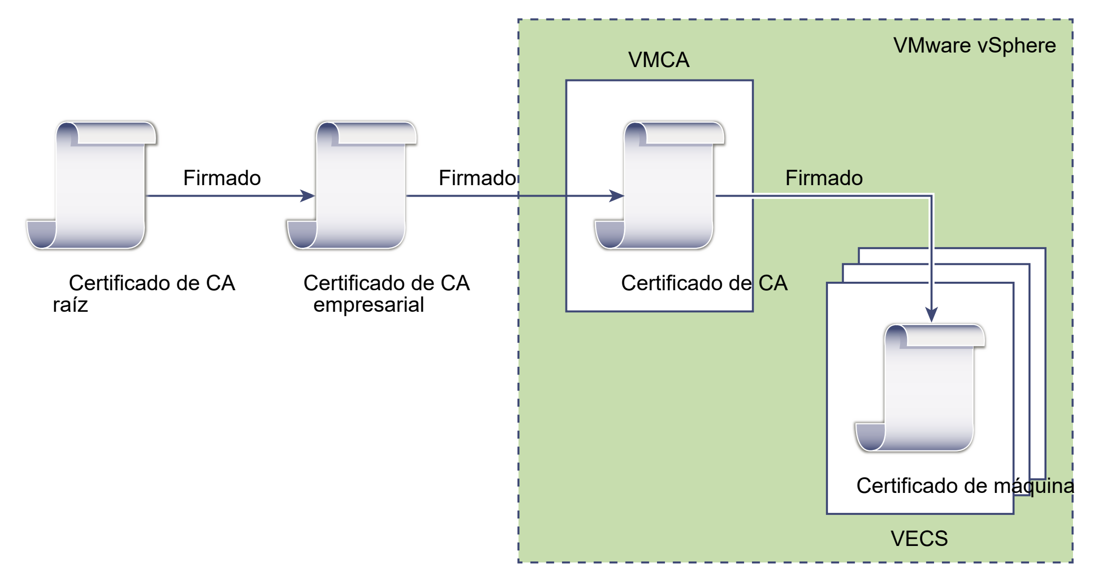
Para obtener información sobre el reemplazo manual de certificados, consulte Reemplazar certificados firmados por VMCA existentes por certificados firmados por VMCA nuevos.

Conversión de VMCA en una CA intermediaria

Puede reemplazar el certificado raíz de VMCA por un certificado firmado por una CA empresarial o externa. VMCA firma el certificado raíz cada vez que aprovisiona certificados, lo que convierte a VMCA en una CA intermediaria.

Nota Si realiza una instalación nueva que incluye una instancia de Platform Services Controller externa, instale el primer Platform Services Controller y reemplace el certificado raíz de VMCA. Luego, instale otros servicios o agregue hosts ESXi al entorno. Si realiza una instalación nueva que incluye una instancia de Platform Services Controller integrada, reemplace el certificado raíz de VMCA antes de agregar hosts ESXi. Si lo hace, VMCA firma toda la cadena y no es necesario generar certificados nuevos.

Figura 3-2. Los certificados firmados por una CA empresarial o externa usan VMCA como CA intermediaria



Puede usar las siguientes opciones de vSphere Certificate Manager:

- Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados
- Reemplazo de un certificado de SSL de una máquina con un certificado de VMCA (implementación de varios nodos)
- Reemplazo de un certificado de un usuario de una solución con un certificado de VMCA (implementación de varios nodos)

Para obtener información sobre el reemplazo manual de certificados, consulte Utilizar VMCA como entidad de certificación intermedia.

No use VMCA; aprovisione certificados personalizados

Puede reemplazar los certificados firmados por VMCA existentes con certificados personalizados. Si emplea este enfoque, asume la responsabilidad del aprovisionamiento y la supervisión de todos los certificados.

Figura 3-3. Certificados externos que se almacenan directamente en VECS

Puede usar las siguientes opciones de vSphere Certificate Manager:

- Reemplazar un certificado SSL de máquina por un certificado personalizado
- Reemplazar los certificados de usuarios de soluciones con certificados personalizados

Para obtener información sobre el reemplazo manual de certificados, consulte Usar certificados personalizados con vSphere.

También puede utilizar vSphere Client a fin de generar una CSR para un certificado SSL de máquina (personalizado) y reemplazar el certificado después de que la entidad de certificación lo devuelve. Consulte Generar una solicitud de firma del certificado para el certificado SSL de máquina con vSphere Client (certificados personalizados).

Implementación híbrida

Puede hacer que VMCA proporcione algunos de los certificados, pero, al mismo tiempo, certificados personalizados para otras partes de la infraestructura. Por ejemplo, dado que los certificados de usuarios de soluciones se usan solo para autenticar vCenter Single Sign-On, considere la posibilidad de hacer que VMCA aprovisione esos certificados. Reemplace los certificados de SSL de máquinas con certificados personalizados para proteger todo el tráfico de SSL.

Con frecuencia, la directiva de la empresa no permite CA intermedias. En esos casos, la implementación híbrida es una buena solución. Minimiza la cantidad de certificados que deben reemplazarse y protege todo el tráfico. La implementación híbrida solo deja tráfico interno, es decir, tráfico del usuario de la solución, para usar los certificados predeterminados firmados por VMCA.

Reemplazar certificados de ESXi

Para los hosts ESXi, puede cambiar el comportamiento de aprovisionamiento de certificados desde vSphere Client. Consulte la documentación de *Seguridad de vSphere* para obtener detalles.

Tabla 3-4. Opciones de reemplazo de certificados de ESXi

Opción	Descripción
Modo VMware Certificate Authority (valor predeterminado)	Cuando se renuevan certificados desde vSphere Client, VMCA emite los certificados para los hosts. Si cambió el certificado raíz de VMCA para incluir una cadena de certificados, los certificados del host incluyen la cadena completa.
Modo de entidad de certificación personalizada	Permite actualizar y usar manualmente certificados que no han sido firmados o emitidos por VMCA.
Modo de huella digital	Puede usarse para conservar los certificados de la versión 5.5 durante la actualización. Use este modo únicamente de manera temporal en situaciones de depuración.

Casos en que vSphere utiliza certificados

En vSphere 6.0 y versiones posteriores, VMware Certificate Authority (VMCA) aprovisiona el entorno con certificados. Entre ellos se encuentran certificados SSL de equipos para conexiones seguras, certificados de usuarios de solución para la autenticación de servicios ante vCenter Single Sign-On y certificados para hosts ESXi.

Los siguientes certificados están en uso.

Tabla 3-5. Certificados en vSphere 6.0 y versiones posteriores

Certificado	Aprovisionado	Comentarios
Certificados de ESXi	VMCA (valor predeterminado)	Almacenados localmente en el host ESXi
Certificados SSL de máquina	VMCA (valor predeterminado)	Almacenados en VECS
Certificados de usuarios de solución	VMCA (valor predeterminado)	Almacenados en VECS

Tabla 3-5. Certificados en vSphere 6.0 y versiones posteriores (continuación)

Certificado	Aprovisionado	Comentarios
Certificado de firma SSL vCenter Single Sign-On	Aprovisionado durante la instalación.	Administre este certificado desde vSphere Web Client. **Nota** No cambie este certificado en el sistema de archivos, ya que podría producirse un comportamiento impredecible.
Certificado SSL de VMware Directory Service (VMDIR)	Aprovisionado durante la instalación.	A partir de vSphere 6.5, el certificado SSL del equipo se usa como certificado de vmdir.

ESXi

Los certificados de ESXi se almacenan localmente en cada host del directorio `/etc/vmware/ssl`. Los certificados de ESXi son aprovisionados por VMCA de manera predeterminada, pero se pueden utilizar certificados personalizados. Los certificados de ESXi se aprovisionan cuando se agrega el host por primera vez a vCenter Server y cuando el host se vuelve a conectar.

Certificados SSL de máquina

El certificado SSL de máquina de cada nodo se utiliza para crear un socket de SSL en el lado del servidor. Los clientes SSL se conectan con el socket SSL. El certificado se utiliza para comprobar el servidor y establecer una comunicación segura mediante los protocolos HTTPS o LDAPS.

Cada nodo tiene su propio certificado SSL de máquina. Los nodos incluyen instancias de vCenter Server, instancias de Platform Services Controller o instancias de implementación integradas. Todos los servicios que se ejecutan en un nodo utilizan el certificado SSL de máquina para exponer sus endpoints SSL.

Los siguientes servicios utilizan el certificado SSL de máquina.

- El servicio de proxy inverso en cada nodo de Platform Services Controller. Las conexiones SSL a los servicios individuales de vCenter siempre van al proxy inverso. El tráfico no va a los servicios en sí.
- El servicio de vCenter (vpxd) en los nodos de administración y los nodos integrados.
- VMware Directory Service (vmdir) en los nodos de infraestructura y los nodos integrados.

Los productos de VMware utilizan certificados X.509 versión 3 (X.509v3) estándar para cifrar la información de sesión. La información de sesión se envía mediante SSL entre los componentes.

Certificados de usuarios de solución

Un usuario de solución encapsula uno o varios servicios de vCenter Server. Cada usuario de solución debe estar autenticado en vCenter Single Sign-On. Los usuarios de solución utilizan certificados para autenticar vCenter Single Sign-On a través del intercambio de token SAML.

Un usuario de solución presenta el certificado ante vCenter Single Sign-On cuando debe autenticarse por primera vez, después de un reinicio y de transcurrido un tiempo de espera. El tiempo de espera (tiempo de espera Holder-of-Key) puede establecerse desde vSphere Web Client y su valor predeterminado es 2.592.000 segundos (30 días).

Por ejemplo, el usuario de solución vpxd presenta su certificado en vCenter Single Sign-On al conectarse a vCenter Single Sign-On. El usuario de solución vpxd recibe un token SAML de vCenter Single Sign-On y, a continuación, puede utilizarlo para autenticarse en otros servicios y usuarios de solución.

Los siguientes almacenes de certificados de usuarios de solución se incluyen en VECS en cada nodo de administración y en cada implementación integrada:

- `machine`: lo utilizan el servidor de licencias y el servicio de registro.

  Nota El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina.

- `vpxd`: almacén de daemon del servicio vCenter (vpxd) de los nodos de administración y las implementaciones integradas. vpxd utiliza el certificado de usuario de solución que está en este almacén para autenticarse en vCenter Single Sign-On.
- `vpxd-extension`: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución.
- `vsphere-webclient`: almacén de vSphere Web Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento.

Cada nodo de Platform Services Controller incluye un certificado `machine`.

Certificados internos

Los certificados de vCenter Single Sign-On no se almacenan en VECS y no se administran con herramientas de administración de certificados. Como regla general, no es necesario hacer cambios, pero en situaciones especiales, estos certificados se pueden reemplazar.

Certificado de firma de vCenter Single Sign-On

El servicio vCenter Single Sign-On incluye un servicio de proveedor de identidad que emite tokens SAML utilizados para la autenticación en todo el sistema vSphere. Un token SAML representa la identidad del usuario y, a su vez, contiene información sobre la pertenencia a los grupos. Cuando vCenter Single Sign-On emite tokens SAML, firma cada token con su certificado de firma, de modo que los clientes de vCenter Single Sign-On pueden comprobar que el token SAML proviene de un origen confiable.

vCenter Single Sign-On emite tokens SAML HoK para los usuarios de solución y tokens de portador para otros usuarios, que inician sesión con un nombre de usuario y una contraseña.

Este certificado se puede reemplazar desde vSphere Web Client. Consulte Actualizar el certificado del servicio de token de seguridad.

Certificado SSL de VMware Directory Service

A partir de vSphere 6.5, el certificado SSL del equipo se usa como certificado de directorio de VMware. Para versiones anteriores de vSphere, consulte la documentación correspondiente.

Certificados de cifrado de máquinas virtuales de vSphere

La solución de cifrado de máquinas virtuales de vSphere se conecta con un servidor de administración de claves (Key Management Server, KMS) externo. Según la manera en que la solución se autentique ante el KMS, puede generar certificados y almacenarlos en VECS. Consulte la documentación de *Seguridad de vSphere*.

Servicios básicos de identidad de VMware y VMCA

Los servicios básicos de identidad forman parte de toda implementación integrada y todo nodo de servicios de plataforma. VMCA forma parte de cada grupo de servicios básicos de identidad de VMware. Utilice las CLI de administración y vSphere Client para interactuar con estos servicios.

Los servicios básicos de identidad de VMware incluyen varios componentes.

Tabla 3-6. Servicios básicos de identidad

Servicio	Descripción	Incluido en
VMware Directory Service (vmdir)	Controla la administración de certificados SAML para la autenticación con vCenter Single Sign-On.	Platform Services Controller Implementación integrada
VMware Certificate Authority (VMCA)	Emite certificados para usuarios de soluciones de VMware, certificados para las máquinas en las que se ejecutan servicios y certificados para hosts ESXi. VMCA puede utilizarse en el estado en que se encuentra o como entidad de certificación intermediaria. VMCA emite certificaciones únicamente a los clientes que pueden autenticarse en vCenter Single Sign-On en el mismo dominio.	Platform Services Controller Implementación integrada
VMware Authentication Framework Daemon (VMAFD)	Incluye VMware Endpoint Certificate Store (VECS) y otros servicios de autenticación. Los administradores de VMware interactúan con VECS; los otros servicios son de uso interno.	Platform Services Controller vCenter Server Implementación integrada

Descripción general de VMware Endpoint Certificate Store

VMware Endpoint Certificate Store (VECS) sirve de repositorio local (del lado del cliente) para certificados, claves privadas y cualquier información de certificados que pueda guardarse en un almacén de claves. Puede optar por no usar VMCA como entidad de certificación y firmante de certificados, pero debe usarlo para almacenar todos los certificados, las claves y demás elementos de vCenter. Los certificados de ESXi se almacenan de forma local en cada host y no en VECS.

VECS se ejecuta como parte de VMware Authentication Framework Daemon (VMAFD). VECS se ejecuta en todas las implementaciones integradas, el nodo de Platform Services Controller y el nodo de administración, y conserva todos los almacenes de claves que contienen certificados y claves.

VECS sondea VMware Directory Service (vmdir) de forma periódica en busca de actualizaciones del almacén raíz de confianza. También puede administrar certificados de forma explícita en VECS mediante los comandos `vecs-cli`. Consulte Referencia de comandos vecs-cli.

VECS incluye los siguientes almacenes.

Tabla 3-7. Almacenes en VECS

Almacén	Descripción
Almacén SSL de máquina (MACHINE_SSL_CERT)	■ El servicio de proxy inverso lo utiliza en cada nodo de vSphere. ■ VMware Directory Service (vmdir) lo utiliza en implementaciones integradas y en cada nodo de Platform Services Controller. Todos los servicios de vSphere 6.0 y versiones posteriores se comunican mediante un proxy inverso que utiliza el certificado SSL de equipo. Por razones de compatibilidad con versiones anteriores, los servicios de la versión 5.x todavía utilizan puertos específicos. Como resultado, algunos servicios como vpxd todavía tienen su propio puerto abierto.
Almacén raíz de confianza (TRUSTED_ROOTS)	Contiene todos los certificados raíz de confianza.

Tabla 3-7. Almacenes en VECS (continuación)

Almacén	Descripción
Almacenes de usuarios de solución ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient	VECS incluye un almacén para cada usuario de solución. El asunto de cada certificado de usuario de solución debe ser único, por ejemplo, el certificado de máquina no puede tener el mismo asunto que el certificado de vpxd. Los certificados de usuarios de solución se utilizan para la autenticación con vCenter Single Sign-On. vCenter Single Sign-On comprueba que el certificado sea válido, pero no comprueba otros atributos del certificado. En una implementación integrada, todos los certificados de usuarios de solución están en el mismo sistema. Los siguientes almacenes de certificados de usuarios de solución se incluyen en VECS en cada nodo de administración y en cada implementación integrada: ■ machine: lo utilizan el servidor de licencias y el servicio de registro. **Nota** El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina. ■ vpxd: almacén de daemon del servicio vCenter (vpxd) de los nodos de administración y las implementaciones integradas. vpxd utiliza el certificado de usuario de solución que está en este almacén para autenticarse en vCenter Single Sign-On. ■ vpxd-extension: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución. ■ vsphere-webclient: almacén de vSphere Web Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento. Cada nodo de Platform Services Controller incluye un certificado machine.

Tabla 3-7. Almacenes en VECS (continuación)

Almacén	Descripción
Almacén de copias de seguridad de la utilidad vSphere Certificate Manager (BACKUP_STORE)	VMCA (VMware Certificate Manager) lo utiliza para admitir la reversión de certificados. Solo el estado más reciente se almacena como copia de seguridad; no se puede volver más de un paso.
Otros almacenes	Las soluciones pueden agregar otros almacenes. Por ejemplo, la solución Virtual Volumes agrega un almacén SMS. No modifique los certificados de estos almacenes a menos que así se indique en la documentación de VMware o en un artículo de la base de conocimientos de VMware. **Nota** La eliminación del almacén TRUSTED_ROOTS_CRLS puede dañar la infraestructura de certificado. No elimine ni modifique el almacén TRUSTED_ROOTS_CRLS.

El servicio de vCenter Single Sign-On almacena el certificado de firma de tokens y su certificado SSL en el disco. Puede cambiar el certificado de firma de tokens desde vSphere Client.

Algunos certificados se almacenan en el sistema de archivos, ya sea de forma temporal durante el inicio o de forma permanente. No cambie los certificados en el sistema de archivos. Use `vecs-cli` para realizar operaciones en los certificados almacenados en VECS.

Nota No cambie ningún archivo de certificado en el disco a menos que se indique en la documentación de VMware o en los artículos de la base de conocimientos. De lo contrario, se puede producir un comportamiento inesperado.

Administrar la revocación de certificados

Si sospecha que la confiabilidad de uno de los certificados está comprometida, reemplace todos los certificados actuales, incluido el certificado raíz de VMCA.

vSphere 6.0 admite el reemplazo de los certificados, pero no aplica su revocación en los hosts ESXi o en los sistemas vCenter Server.

Quite los certificados revocados de todos los nodos. Si no los quita, un ataque de tipo "Man in the middle" (intermedio) podría comprometerlos al habilitarse una suplantación con las credenciales de la cuenta.

Reemplazar certificados en implementaciones de gran tamaño

El reemplazo de certificados en implementaciones que incluyen varios nodos de administración y uno o más nodos de Platform Services Controller es similar al reemplazo en implementaciones integradas. En ambos casos, puede usar la utilidad vSphere Certificate Management o reemplazar los certificados a mano. Algunas prácticas recomendadas sirven como guía para el proceso de reemplazo.

Reemplazar certificados en entornos de alta disponibilidad que incluyen un equilibrador de carga

Por lo general, en los entornos con menos de ocho sistemas vCenter Server, se implementa una única instancia de Platform Services Controller y un servicio vCenter Single Sign-On asociado. En los entornos más grandes, considere la posibilidad de usar varias instancias de Platform Services Controller, protegidas por un equilibrador de carga. En el informe técnico *Guía de implementación de vCenter Server 6.0*, disponible en el sitio web de VMware, se describe esta configuración.

Reemplazo de certificados SSL de máquina en entornos con varios nodos de administración

Si el entorno incluye varios nodos de administración y una única instancia de Platform Services Controller, puede reemplazar los certificados con vSphere Client o la utilidad vSphere Certificate Manager, o bien hacerlo manualmente con los comandos de la CLI de vSphere.

vSphere Certificate Manager

Ejecute vSphere Certificate Manager en cada máquina. En los nodos de administración, se le solicitará la dirección IP de Platform Services Controller. Según la tarea que realice, también se le solicitará información del certificado.

Reemplazar certificados de forma manual

Para reemplazar un certificado manualmente, ejecute los comandos de reemplazo de los certificados en cada máquina. En los nodos de administración, debe especificar Platform Services Controller con el parámetro `--server`. Consulte los siguientes temas para obtener más detalles:

- Reemplazar certificados SSL de máquina por certificados firmados por VMCA
- Reemplazar certificados SSL de máquina (entidad de certificación intermedia)
- Reemplazar certificados SSL de máquina por certificados personalizados

Reemplazo de certificados del usuario de solución en entornos con varios nodos de administración

Si el entorno incluye varios nodos de administración y una única instancia de Platform Services Controller, siga estos pasos para reemplazar los certificados.

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

vSphere Certificate Manager

Ejecute vSphere Certificate Manager en cada máquina. En los nodos de administración, se le solicitará la dirección IP de Platform Services Controller. Según la tarea que realice, también se le solicitará información del certificado.

Reemplazar certificados de forma manual

1 Genere o solicite un certificado. Necesita los siguientes certificados:

   - Un certificado para el usuario de solución de la máquina en Platform Services Controller.
   - Un certificado para el usuario de solución de la máquina en cada nodo de administración.
   - Un certificado para cada uno de los siguientes usuarios de solución en cada nodo de administración:
     - usuario de `vpxd solution`
     - usuario de la solución `vpxd-extension`
     - usuario de la solución `vsphere-webclient`

2 Reemplace los certificados en cada nodo. El proceso en particular depende del tipo de reemplazo de certificados que esté realizando. Consulte Administrar certificados con la utilidad vSphere Certificate Manager.

Consulte los siguientes temas para obtener más detalles:

- Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA
- Reemplazar certificados de usuarios de solución (entidad de certificación intermedia)
- Reemplazar los certificados de usuarios de soluciones con certificados personalizados

Reemplazar certificados en entornos que incluyen soluciones externas

Algunas soluciones, como VMware vCenter Site Recovery Manager o VMware vSphere Replication, siempre se instalan en una máquina diferente que el sistema de vCenter Server o Platform Services Controller. Si se reemplaza el certificado SSL predeterminado de una máquina en el sistema vCenter Server o Platform Services Controller, se produce un error de conexión cuando la solución intenta conectarse al sistema vCenter Server.

Es posible ejecutar el script `ls_update_certs` para solucionar el problema. Consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2109074 para obtener más información.

Administrar certificados con vSphere Client

Puede ver y administrar certificados mediante vSphere Client. También puede realizar muchas tareas de administración de certificados con la utilidad vSphere Certificate Manager.

vSphere Client le permite realizar estas tareas de administración.

- Ver los certificados SSL y los certificados raíz de confianza.
- Renovar los certificados actuales o reemplazarlos.
- Generar una solicitud de firma del certificado (Certificate Signing Request, CSR) personalizada para un certificado SSL de máquina y reemplazar el certificado cuando la entidad de certificación lo devuelva.

La mayor parte de los flujos de trabajo de reemplazo de certificados se admite completamente desde vSphere Client. Para generar CSR para los certificados SSL de máquina, puede utilizar vSphere Client o la utilidad Certificate Manage.

Flujos de trabajos compatibles

Después de instalar una instancia de Platform Services Controller, VMware Certificate Authority en ese nodo aprovisiona todos los demás nodos del entorno con certificados predeterminados. Consulte Capítulo 3 Certificados de seguridad de vSphere para obtener sugerencias acerca de las recomendaciones actuales para la administración de certificados.

Se puede utilizar cualquiera de los siguientes flujos de trabajo para renovar o reemplazar certificados.

Renovar certificados

Puede hacer que VMCA renueve los certificados de usuario de solución y SSL en el entorno desde vSphere Client.

Conversión de VMCA en una CA intermediaria

Puede generar una CSR mediante la utilidad vSphere Certificate Manager. Después puede editar el certificado que recibe de CSR para que se agregue VMCA a la cadena y, a continuación, agregar la cadena de certificados y la clave privada al entorno. Al renovar todos los certificados, VMCA aprovisiona todas las máquinas y los usuarios de la solución con certificados firmados por la cadena completa.

Reemplazar certificados por certificados personalizados

Si no desea utilizar VMCA, puede generar CSR para los certificados que desea reemplazar. La CA devuelve un certificado raíz y un certificado firmado para cada CSR. Se puede cargar el certificado raíz y los certificados personalizados desde Platform Services Controller.

Nota Si utiliza VMCA como una entidad de certificación intermedia o utiliza certificados personalizados, es posible que experimente una complejidad considerable y que exista la posibilidad de un impacto negativo para la seguridad, así como un aumento innecesario en el riesgo operativo. Para obtener más información sobre la administración de certificados en un entorno de vSphere, consulte la publicación de blog llamada *Revisión de producto nuevo: reemplazo del certificado SSL de vSphere híbrido* en http://vmware.com/go/hybridvmca.

En un entorno de modo mixto, se pueden usar los comandos de la CLI para reemplazar el certificado de vCenter Single Sign-On después de reemplazar los otros certificados. Consulte Reemplazar el certificado de VMware Directory Service en entornos de modo mixto.

Explorar los almacenes de certificados desde vSphere Client

En cada nodo de Platform Services Controller y en cada nodo de vCenter Server se incluye una instancia de VMware Endpoint Certificate Store (VECS). Puede explorar los diferentes almacenes en VMware Endpoint Certificate Store desde vSphere Client.

Consulte Descripción general de VMware Endpoint Certificate Store para obtener detalles sobre los diferentes almacenes incluidos en VECS.

Requisitos previos

Para la mayoría de las tareas de administración, debe contar con la contraseña del administrador de la cuenta de dominio local, administrator@vsphere.local o un dominio diferente si cambió el dominio durante la instalación.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Introduzca las credenciales de vCenter Server.

5 Explore los certificados almacenados en VMware Endpoint Certificate Store (VECS).

   Descripción general de VMware Endpoint Certificate Store explica qué hay en los almacenes individuales.

6 Para ver detalles sobre el certificado, seleccione el certificado y haga clic en **Ver detalles**.

7 Utilice el menú **Acciones** para renovar o reemplazar los certificados.

   Por ejemplo, si reemplaza el certificado existente, puede quitar el certificado raíz anterior posteriormente. Quite los certificados únicamente si está seguro de que ya no están en uso.

Establecer el umbral para las advertencias de caducidad de certificados de vCenter

A partir de vSphere 6.0, vCenter Server supervisa todos los certificados de VMware Endpoint Certificate Store (VECS) y emite una alarma cuando un certificado está a 30 días o menos de

caducar. Puede cambiar el tiempo de anticipación con el que desea recibir el alerta con la opción avanzada `vpxd.cert.threshold`.

Procedimiento

1 Inicie sesión en vSphere Client.

2 Seleccione el objeto vCenter Server y haga clic en **Configurar**.

3 Haga clic en **Configuración avanzada**.

4 Haga clic en **Editar configuración** y filtre por **`umbral`**.

5 Cambie la configuración de `vpxd.cert.threshold` al valor deseado y haga clic en **Guardar**.

Reemplazar certificados por nuevos certificados firmados por VMCA desde vSphere Client

Todos los certificados firmados por VMCA se pueden reemplazar por nuevos certificados firmados por VMCA. Este proceso se denomina "renovación de certificados". Puede renovar los certificados seleccionados o todos los certificados del entorno desde vSphere Client.

Requisitos previos

Para la administración de certificados, debe proporcionar la contraseña del administrador del dominio local (administrator@vsphere.local de forma predeterminada). Si está renovando certificados para un sistema vCenter Server, también puede proporcionar las credenciales de vCenter Single Sign-On para un usuario con privilegios de administrador en el sistema vCenter Server.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Introduzca las credenciales de vCenter Server.

5 Renueve el certificado SSL de máquina del sistema local.

   a Seleccione **Certificado SSL de máquina**.

   b Haga clic en **Acciones > Renovar**.

   c Haga clic en **Renovar**.

   Aparece un mensaje que reza que se renueva el certificado.

6 (Opcional) Renueve los certificados de usuarios de solución para el sistema local.

   a En **Certificados de solución**, seleccione un certificado.

   b Haga clic en **Acciones > Renovar** para renovar los certificados individuales seleccionados o haga clic en **Renovar todo** para renovar todos los certificados de los usuarios de solución.

   Aparece un mensaje que reza que se renueva el certificado.

7 Si el entorno incluye una instancia externa de Platform Services Controller, es posible renovar los certificados para cada sistema vCenter Server.

   a Haga clic en el botón **Cerrar sesión** en el panel Administración de certificados.

   b Cuando se lo solicite el sistema, especifique la dirección IP o el FQDN del sistema vCenter Server y el nombre de usuario y la contraseña del administrador de vCenter Server que se puede autenticar en vCenter Single Sign-On.

   c Renueve el certificado SSL de máquina en vCenter Server y, de manera opcional, cada certificado de usuario de solución.

   d Si existen varios sistemas vCenter Server en el entorno, repita el proceso para cada sistema.

Pasos siguientes

Reinicie los servicios de Platform Services Controller. Puede reiniciar la instancia de Platform Services Controller o ejecutar los siguientes comandos desde la línea de comandos:

Windows

En Windows, el comando `service-control` está ubicado en *`VCENTER_INSTALL_PATH`*`\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

Configurar el sistema para utilizar certificados personalizados desde Platform Services Controller

Puede utilizar Platform Services Controller para configurar el entorno de manera que utilice certificados personalizados.

Puede generar Solicitudes de firma de certificados (CSR) para cada máquina y para cada usuario de la solución que use la utilidad Administrador de certificados. También puede generar CSR para cada máquina y reemplazar los certificados al recibirlos de la entidad de certificación (Certificate Authority, CA) de terceros mediante vSphere Client. Cuando entrega las CSR a su CA interna o externa, la CA devuelve certificados firmados y el certificado raíz. Se puede cargar el certificado raíz y los certificados firmados desde la UI de Platform Services Controller.

Generar una solicitud de firma del certificado para el certificado SSL de máquina con vSphere Client (certificados personalizados)

El certificado SSL de máquina se utiliza en el servicio de proxy inverso de cada nodo de administración, en Platform Services Controller y en la implementación integrada. Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. Puede utilizar vSphere Client para generar una solicitud de firma del certificado (CSR) para el certificado SSL de máquina y reemplazar el certificado una vez que esté listo.

Requisitos previos

El certificado debe cumplir con los siguientes requisitos:

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Contiene los siguientes usos de claves: firma digital, cifrado de clave

Nota No utilice los puntos de distribución de CRL, el acceso a la información de autoridad o la información de la plantilla de certificado en ningún certificado personalizado.

La generación de una CSR para el certificado SSL solo se admite en vCenter Server Appliance. No se admite en una instalación de Windows de vCenter Server.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Introduzca las credenciales de vCenter Server.

5 Genere la CSR.

   a En **Certificado SSL de máquina**, para el certificado que desea reemplazar, haga clic en **Acciones > Generar solicitud de firma del certificado (CSR)**.

   b Introduzca la información del certificado y haga clic en **Siguiente**.

   c Copie o descargue la CSR.

   d Haga clic en **Finalizar**.

   e Proporcione la CSR a su entidad de certificación.

Pasos siguientes

Cuando la entidad de certificación devuelve el certificado, reemplace el certificado existente en el almacén de certificados. Consulte Agregar certificados personalizados desde Platform Services Controller.

Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados)

Es posible utilizar vSphere Certificate Manager para generar solicitudes de firma de certificado (CSR) y, a continuación, enviarlas a la entidad de certificación empresarial o a una entidad de certificación externa. Los certificados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

Puede ejecutar la herramienta Certificate Manager en la línea de comandos de la siguiente manera:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Requisitos previos

vSphere Certificate Manager solicita información. La solicitud depende del entorno y del tipo de certificado que se desea reemplazar.

- Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.

- Cuando se desea generar una CSR en un entorno con una instancia externa de Platform Services Controller, se solicita el nombre de host o la dirección IP de Platform Services Controller.
- Para generar una CSR para un certificado SSL de máquina, se solicitan las propiedades del certificado, que están almacenadas en el archivo `certool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.

Procedimiento

1 En cada máquina del entorno, inicie vSphere Certificate Manager y seleccione la opción 1.

2 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.

3 Seleccione la opción 1 para generar la CSR, responda las solicitudes del sistema y salga de Certificate Manager.

   Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

4 Si también desea reemplazar todos los certificados de usuario de solución, reinicie Certificate Manager.

5 Seleccione la opción 5.

6 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.

7 Seleccione la opción 1 para generar las CSR, responda las solicitudes del sistema y salga de Certificate Manager.

   Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

   En cada nodo de Platform Services Controller, Certificate Manager generará un certificado y un par de claves. En cada nodo de vCenter Server, Certificate Manager generará cuatro certificados y pares de claves.

Pasos siguientes

Realice el reemplazo de certificados.

Agregar un certificado raíz de confianza al almacén de certificados

Si desea utilizar certificados de terceros en su entorno, debe agregar un certificado raíz de confianza al almacén de certificados.

Requisitos previos

Obtenga el certificado raíz personalizado de la entidad de certificación interna o de terceros.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Introduzca las credenciales de vCenter Server.

5 En **Certificados raíz de confianza**, haga clic en **Agregar**.

6 Haga clic en **Examinar** y seleccione la ubicación de la cadena de certificados.

   Puede usar un archivo del tipo CER, PEM o CRT.

7 Haga clic en **Agregar**.

   El certificado se agrega al almacén.

Pasos siguientes

Reemplace los certificados SSL de equipo y, opcionalmente, los certificados de usuarios de solución con certificados que firmó esta entidad de certificación.

Agregar certificados personalizados desde Platform Services Controller

Los certificados SSL de máquina y los certificados de usuarios de solución se pueden agregar al almacén de certificados desde Platform Services Controller

En la mayoría de los casos, reemplazar el certificado SSL de máquina para cada componente es suficiente. El certificado de usuarios de solución permanece detrás de un proxy.

Requisitos previos

Genere solicitudes de firma de certificado (CSR) para cada certificado que desea reemplazar. Las CSR se pueden generar mediante la utilidad Certificate Manager. También puede generar una CSR para un certificado SSL de máquina mediante vSphere Client. Coloque el certificado y la clave privada en una ubicación accesible para Platform Services Controller.

Procedimiento

1 Inicie sesión con vSphere Client en la instancia de vCenter Server conectada a Platform Services Controller.

2 Especifique el nombre de usuario y la contraseña para administrator@vsphere.local u otro miembro del grupo de administradores de vCenter Single Sign-On.

   Si especificó otro dominio durante la instalación, inicie sesión como administrator@*mydomain*.

3 Desplácese hasta la interfaz de usuario de administración de certificados.

   a En el menú **Inicio**, seleccione **Administración**.

   b En **Certificados**, haga clic en **Administración de certificados**.

4 Introduzca las credenciales de vCenter Server.

5 Para reemplazar un certificado SSL de máquina, siga estos pasos:

   a En **Certificado SSL de máquina**, para el certificado que se desea reemplazar, haga clic en **Acciones > Reemplazar**.

   b Busque el certificado SSL de máquina (archivo `.cer`, `.pem` o `.crt`) y la clave privada (archivo `.key`).

   c Haga clic en **Reemplazar**.

6 Para reemplazar los certificados de usuarios de solución, siga estos pasos:

   a En **Certificados de solución**, para el primero de los certificados de un componente, por ejemplo, **equipo**, haga clic en **Acciones > Reemplazar**.

   b Haga clic en **Examinar** para reemplazar la cadena de certificados; a continuación, haga clic en **Examinar** para reemplazar la clave privada.

   c Haga clic en **Reemplazar**.

   d Repita el proceso para los otros certificados del mismo componente.

Resultados

Se muestra un mensaje que indica que se reemplazó el certificado.

Pasos siguientes

Reinicie los servicios de Platform Services Controller. Puede reiniciar la instancia de Platform Services Controller o ejecutar los siguientes comandos desde la línea de comandos:

Windows

En Windows, el comando `service-control` está ubicado en *`VCENTER_INSTALL_PATH`*`\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

Administrar certificados desde vSphere Web Client

Puede consultar certificados desde vSphere Web Client. Realice todas las demás tareas de administración desde vSphere Client.

Consulte Administrar certificados con vSphere Client.

Ver certificados de vCenter con vSphere Web Client

Es posible ver los certificados que conoce vCenter Certificate Authority (VMCA) para determinar si los certificados activos están por caducar, comprobar los certificados caducados y ver el estado del certificado raíz. Todas las tareas de administración de certificados se realizan con las CLI de administración de certificados.

Los certificados asociados se ven con la instancia de VMCA que se incluye con la implementación integrada o con Platform Services Controller. La información de certificados se replica en todas las instancias de VMware Directory Service (vmdir).

Cuando se intentan ver certificados en vSphere Web Client, se solicitan un nombre de usuario y una contraseña. Especifique el nombre de usuario y la contraseña de un usuario con privilegios para VMware Certificate Authority, es decir, un usuario que esté en el grupo Administradores de CA de vCenter Single Sign-On.

Procedimiento

1 Inicie sesión con vSphere Web Client en vCenter Server como administrator@vsphere.local u otro usuario del grupo Administradores de CA de vCenter Single Sign-On.

2 En el menú Inicio, seleccione **Administración**.

3 Haga clic en **Implementación > Configuración del sistema**.

4 Haga clic en **Nodos** y seleccione un host en la lista **Nodos**.

5 Haga clic en la pestaña **Administrar** y en **Entidad de certificación**.

6 Haga clic en el tipo de certificado para el que desea ver información.

Opción	Descripción
Certificados activos	Muestra los certificados activos, incluida su información de validación. El icono verde Válido hasta cambia cuando el certificado está por caducar.
Certificados revocados	Muestra la lista de certificados revocados. No se admite en esta versión.
Certificados caducados	Enumera los certificados caducados.
Certificados raíz	Muestra los certificados raíz disponibles para esta instancia de vCenter Certificate Authority.

7 Seleccione un certificado y haga clic en el botón **Mostrar detalles de certificado** para ver los detalles del certificado.

Los detalles incluyen Nombre de asunto, Emisor, Validez y Algoritmo.

Administrar certificados con la utilidad vSphere Certificate Manager

La utilidad vSphere Certificate Manager permite realizar la mayoría de las tareas de administración de certificados de forma interactiva desde la línea de comandos. vSphere Certificate Manager solicita que se lleve a cabo una tarea, pide las ubicaciones de los certificados y otra información necesaria y, a continuación, detiene e inicia los servicios para reemplazar los certificados.

Si se utiliza vSphere Certificate Manager, el usuario no es responsable de colocar los certificados en VECS (VMware Endpoint Certificate Store) ni de iniciar y detener los servicios.

Antes de ejecutar vSphere Certificate Manager, asegúrese de comprender el proceso de reemplazo y consiga los certificados que desea utilizar.

Precaución vSphere Certificate Manager admite un nivel de reversión. Si se ejecuta vSphere Certificate Manager dos veces y se observa que el entorno se dañó de forma inesperada, la herramienta no puede revertir la primera de las dos ejecuciones.

Ubicación de la utilidad Certificate Manager

La herramienta en la línea de comandos se ejecuta de la siguiente manera:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Procedimiento

1 Opciones de Certificate Manager y flujos de trabajo en este documento

   Puede ejecutar las opciones de Certificate Manager en secuencia para completar un flujo de trabajo. Varias opciones, como la generación de CSR, se utilizan en distintos flujos de trabajo.

2 Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados

   Puede volver a generar el certificado raíz de VMCA para reemplazar el certificado SSL de máquina local, y reemplazar los certificados de usuarios de soluciones locales por certificados firmados por VMCA. En implementaciones de varios nodos, ejecute vSphere Certificate Manager con esta opción en Platform Services Controller y, a continuación, ejecute la utilidad nuevamente en los demás nodos y seleccione `Replace Machine SSL certificate with VMCA Certificate` y `Replace Solution user certificates with VMCA certificates`.

3 Convertir a VMCA en una entidad de certificación intermedia (Certificate Manager)

Es posible convertir a VMCA en una entidad de certificación intermedia si se siguen las solicitudes del sistema desde la utilidad Certificate Manager. Una vez completado el proceso, VMCA firmará todos los certificados nuevos con la cadena completa. Si lo desea, puede utilizar Certificate Manager para reemplazar todos los certificados existentes por nuevos certificados firmados por VMCA.

4 Reemplazar todos los certificados por certificados personalizados (Certificate Manager)

Es posible usar la utilidad vSphere Certificate Manager para reemplazar todos los certificados por certificados personalizados. Antes de iniciar el proceso, es necesario enviar solicitudes de firma de certificado (CSR) a la entidad de certificación. Se puede utilizar Certificate Manager para generar las CSR.

5 Revertir la última operación realizada volviendo a publicar certificados antiguos

Cuando se realiza una operación de administración de certificados mediante vSphere Certificate Manager, primero se almacena el estado actual del certificado en BACKUP_STORE, en VECS, antes del reemplazo de los certificados. Es posible revertir la última operación realizada y regresar al estado anterior.

6 Restablecer todos los certificados

Puede usar la opción `Reset All Certificates` (Restablecer todos los certificados) para reemplazar los certificados de vCenter existentes por los certificados firmados por VMCA.

Opciones de Certificate Manager y flujos de trabajo en este documento

Puede ejecutar las opciones de Certificate Manager en secuencia para completar un flujo de trabajo. Varias opciones, como la generación de CSR, se utilizan en distintos flujos de trabajo.

Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados.

Este flujo de trabajo de una sola opción (opción 2) puede usarse de manera independiente o como parte del flujo de trabajo de certificado intermedio. Consulte Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados.

Convertir a VMCA en una entidad de certificación intermedia

Para hacer que VMCA sea una CA intermedia, debe ejecutar Certificate Manager varias veces. El flujo de trabajo ofrece el conjunto completo de pasos para reemplazar los certificados SSL de máquina y los certificados de usuarios de soluciones. Explica qué hacer en entornos con instancias integradas de Platform Services Controller o instancias externas de Platform Services Controller.

1 Para generar una CSR, seleccione la opción 2, Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados. A continuación, debe introducir algunos datos sobre el certificado. Cuando se le solicite nuevamente una opción, seleccione la opción 1.

Envíe la CSR a la CA externa o de la empresa. Recibirá un certificado firmado y un certificado raíz de la CA.

2 Combine el certificado raíz de VMCA con el certificado raíz de CA y guarde el archivo.

3 Seleccione la opción 2, Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados. Este proceso reemplaza todos los certificados en el equipo local.

4 En una implementación de varios nodos, debe reemplazar los certificados en cada nodo.

   a Primero, reemplace el certificado SSL de la máquina con el (nuevo) certificado de VMCA (opción 3).

   b A continuación, reemplace los certificados de usuarios de soluciones con el (nuevo) certificado de VMCA (opción 6).

Consulte Convertir a VMCA en una entidad de certificación intermedia (Certificate Manager).

Reemplazar todos los certificados por certificados personalizados

Para reemplazar todos los certificados por certificados personalizados, debe ejecutar Certificate Manager varias veces. El flujo de trabajo ofrece el conjunto completo de pasos para reemplazar los certificados SSL de máquina y los certificados de usuarios de soluciones. Explica qué hacer en entornos con instancias integradas de Platform Services Controller o instancias externas de Platform Services Controller.

1 Se generan solicitudes de firma del certificado para el certificado SSL de máquina y los certificados de usuarios de soluciones por separado en cada equipo.

   a Para generar CSR del certificado SSL de máquina, seleccione la opción 1.

   b Si la directiva de la compañía requiere el reemplazo de todos los certificados, también debe seleccionar la opción 5.

2 Después de recibir los certificados firmados y el certificado raíz de la CA, debe reemplazar el certificado SSL en cada equipo con la opción 1.

3 Si además desea reemplazar los certificados de usuarios de soluciones, seleccione la opción 5.

4 Por último, en una implementación de varios nodos, debe repetir el proceso en cada nodo.

Consulte Reemplazar todos los certificados por certificados personalizados (Certificate Manager).

Nota A partir de vSphere 6.5, aparece el siguiente mensaje al ejecutar la utilidad Certificate Manager:

```
Enter proper value for VMCA 'Name':
```

Responda al mensaje introduciendo el nombre de dominio completo de la máquina en la que se ejecuta la configuración del certificado.

Regenerar un certificado raíz de VMCA nuevo y reemplazo de todos los certificados

Puede volver a generar el certificado raíz de VMCA para reemplazar el certificado SSL de máquina local, y reemplazar los certificados de usuarios de soluciones locales por certificados firmados por VMCA. En implementaciones de varios nodos, ejecute vSphere Certificate Manager con esta opción en Platform Services Controller y, a continuación, ejecute la utilidad nuevamente en los demás nodos y seleccione `Replace Machine SSL certificate with VMCA Certificate` y `Replace Solution user certificates with VMCA certificates`.

Al reemplazar el certificado SSL de máquina existente por un nuevo certificado firmado por VMCA, vSphere Certificate Manager solicita información e introduce todos los valores, excepto la contraseña y la dirección IP de Platform Services Controller, en el archivo `certool.cfg`.

- Contraseña de administrator@vsphere.local.
- Código de país de dos letras
- Nombre de empresa
- Nombre de organización
- Unidad de organización
- Estado
- Localidad
- Dirección IP (opcional)
- Correo electrónico
- Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
- Dirección IP de Platform Services Controller si ejecuta el comando en un nodo de administración.
- Nombre de VMCA, es decir, el nombre de dominio completo de la máquina en la que se ejecuta la configuración del certificado.

Requisitos previos

Cuando se ejecuta vSphere Certificate Manager con esta opción, se necesita la siguiente información.

- Contraseña de administrator@vsphere.local.
- FQDN de la máquina para la cual se desea generar un nuevo certificado firmado por VMCA. Las demás propiedades tienen los valores predeterminados, pero pueden cambiarse.

Procedimiento

1 Inicie sesión en vCenter Server en una implementación integrada o en una instancia de Platform Services Controller, e inicie vSphere Certificate Manager.

Sistema operativo	Comando
Linux	`/usr/lib/vmware-vmca/bin/certificate-manager`
Windows	`C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat`

2 Seleccione la opción 4,
`Regenerate a new VMCA Root Certificate and replace all certificates.`

3 Responda las solicitudes del sistema.

Certificate Manager generará un nuevo certificado raíz de VMCA en función de su entrada y reemplazará todos los certificados en el sistema donde se ejecuta Certificate Manager. Si se utiliza una implementación integrada, el proceso de reemplazo se completará después de que Certificate Manager haya reiniciado los servicios.

4 Si el entorno contiene una instancia externa de Platform Services Controller, es necesario reemplazar los certificados en cada sistema vCenter Server.

a Inicie sesión en el sistema vCenter Server.

b Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

c Reinicie todos los servicios.

```
service-control --start --all
```

d Para reemplazar el certificado SSL de máquina, ejecute vSphere Certificate Manager con la opción 3, `Replace Machine SSL certificate with VMCA Certificate`.

e Para reemplazar los certificados de usuario de solución, ejecute Certificate Manager con la opción 6, `Replace Solution user certificates with VMCA certificates`.

Convertir a VMCA en una entidad de certificación intermedia (Certificate Manager)

Es posible convertir a VMCA en una entidad de certificación intermedia si se siguen las solicitudes del sistema desde la utilidad Certificate Manager. Una vez completado el proceso, VMCA firmará todos los certificados nuevos con la cadena completa. Si lo desea, puede utilizar Certificate Manager para reemplazar todos los certificados existentes por nuevos certificados firmados por VMCA.

Para hacer que VMCA sea una CA intermedia, debe ejecutar Certificate Manager varias veces. El flujo de trabajo ofrece el conjunto completo de pasos para reemplazar los certificados SSL de máquina y los certificados de usuarios de soluciones. Explica qué hacer en entornos con instancias integradas de Platform Services Controller o instancias externas de Platform Services Controller.

1 Para generar una CSR, seleccione la opción 1, Reemplazar un certificado SSL de máquina por un certificado personalizado y, luego, Opción 1.

   Recibirá un certificado firmado y un certificado raíz de la CA.

2 Combine el certificado raíz de VMCA con el certificado raíz de CA y guarde el archivo.

3 Seleccione la opción 2, Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados. Este proceso reemplaza todos los certificados en el equipo local.

4 En una implementación de varios nodos, debe reemplazar los certificados en cada nodo.

   a En primer lugar, debe reemplazar el certificado SSL de máquina con el (nuevo) certificado de VMCA (opción 3).

   b A continuación, reemplace los certificados de usuarios de soluciones con el (nuevo) certificado de VMCA (opción 6).

Procedimiento

1 Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia)

   Se puede utilizar vSphere Certificate Manager para generar solicitudes de firma del certificado (CSR). Envíe esas CSR a la CA de la empresa o a una entidad de certificación externa para su firma. Los certificados firmados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

2 Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados

Puede utilizar vSphere Certificate Manager para generar una solicitud de firma de certificados (Certificate Signing Requests, CSR) y enviarla a una entidad de certificación de la empresa o de terceros para la firma. A continuación, puede reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados existentes por certificados firmados por la entidad de certificación personalizada.

3 Reemplazar un certificado SSL de máquina por un certificado de VMCA (entidad de certificación intermedia)

En una implementación de varios nodos donde se utiliza VMCA como entidad de certificación intermedia, es necesario reemplazar de forma explícita el certificado SSL de máquina. Primero, se debe reemplazar el certificado raíz de VMCA en el nodo de Platform Services Controller y, a continuación, se pueden reemplazar los certificados en los nodos de vCenter Server para tener la firma de la cadena completa en los certificados. También se puede utilizar esta opción para reemplazar certificados SSL de máquina que se encuentren dañados o a punto de caducar.

4 Reemplazar certificados de usuario de solución por certificados de VMCA (entidad de certificación intermedia)

En un entorno de varios nodos donde se utiliza VMCA como entidad de certificación intermedia, es posible reemplazar de forma explícita los certificados de usuario de solución. Primero, se debe reemplazar el certificado raíz de VMCA en el nodo de Platform Services Controller y, a continuación, se pueden reemplazar los certificados en los nodos de vCenter Server para tener la firma de la cadena completa en los certificados. También se puede utilizar esta opción para reemplazar certificados de usuario de solución que se encuentren dañados o a punto de caducar.

Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia)

Se puede utilizar vSphere Certificate Manager para generar solicitudes de firma del certificado (CSR). Envíe esas CSR a la CA de la empresa o a una entidad de certificación externa para su firma. Los certificados firmados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

- Se puede utilizar vSphere Certificate Manager para crear la CSR.
- Si prefiere crear la CSR de forma manual, el certificado que envíe para firmar debe cumplir con los siguientes requisitos.
  - Tamaño de clave: 2.048 bits o más
  - Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
  - x509 versión 3

- Si utiliza certificados personalizados, la extensión CA debe establecerse con el valor true para certificados de raíz, y el signo cert debe estar en la lista de requisitos.
- La firma CRL debe estar habilitada.
- El uso mejorado de clave puede estar vacío o contener autenticación del servidor.
- No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
- No se admiten los certificados con comodines o con más de un nombre DNS.
- No se pueden crear CA subsidiarias de VMCA.

  Para obtener un ejemplo de uso de la entidad de certificación de Microsoft, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2112009, Crear una plantilla de entidad de certificación de Microsoft para creación de certificados SSL en vSphere 6.0.

Requisitos previos

vSphere Certificate Manager solicita información. Las solicitudes dependen del entorno y del tipo de certificado que se desea reemplazar.

Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.

Procedimiento

1 Ejecute vSphere Certificate Manager.

Sistema operativo	Comando
Windows	`cd "C:\Program Files\VMware\vCenter Server\vmcad"` `certificate-manager`
Linux	`/usr/lib/vmware-vmca/bin/certificate-manager`

2 Seleccione la opción 2.

  Inicialmente, esta opción se utiliza para generar la CSR, no para reemplazar los certificados.

3 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.

4 Seleccione la opción 1 para generar la CSR y responda las solicitudes.

  Es necesario especificar un directorio como parte de este proceso. Certificate Manager coloca el certificado para su firma (archivo `*.csr`) y el archivo de clave correspondiente (archivo `*.key`) en el directorio.

5 Otorgue un nombre a la solicitud de firma del certificado (Certificate Signing Request, CSR) `root_signing_cert.csr`.

6 Envíe la CSR a la empresa o a la CA externa para firmarla y asigne un nombre al certificado firmado `root_signing_cert.cer` resultante.

7 En un editor de texto, combine el certificado de la siguiente manera.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

8 Guarde el archivo como `root_signing_chain.cer`.

Pasos siguientes

Reemplace el certificado raíz existente por el certificado raíz en cadena. Consulte Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados.

Reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazo de todos los certificados

Puede utilizar vSphere Certificate Manager para generar una solicitud de firma de certificados (Certificate Signing Requests, CSR) y enviarla a una entidad de certificación de la empresa o de terceros para la firma. A continuación, puede reemplazar el certificado raíz de VMCA por un certificado de firma personalizado y reemplazar todos los certificados existentes por certificados firmados por la entidad de certificación personalizada.

vSphere Certificate Manager se ejecuta en una instalación integrada o en una instancia externa de Platform Services Controller para reemplazar el certificado raíz de VMCA por un certificado de firma personalizado.

Requisitos previos

- Genere la cadena de certificados.
  - Se puede utilizar vSphere Certificate Manager para crear la solicitud CSR o crear manualmente la CSR.
  - Después de recibir el certificado firmado de la entidad de certificación externa o empresarial, combínelo con el certificado raíz de VMCA inicial para crear la cadena completa.

    Consulte Generar una CSR con vSphere Certificate Manager y preparar certificados raíz (CA intermedia) para conocer los requisitos de certificación y el proceso para combinar los certificados.

- Recopile la información que necesitará.
  - Contraseña de administrator@vsphere.local.
  - Un certificado personalizado válido para la raíz (archivo `.crt`).
  - La clave personalizada válida para la raíz (archivo `.key`).

Procedimiento

1. Inicie vSphere Certificate Manager en una instalación integrada o en una instancia de Platform Services Controller externa y seleccione la opción 2.
2. Seleccione nuevamente la opción 2 para iniciar el reemplazo de certificados y responder a las solicitudes.
   a. Especifique la ruta de acceso completa al certificado raíz cuando se le solicite.
   b. Si es la primera vez que reemplaza los certificados, se le solicitará información que se utilizará para el certificado SSL de máquina.

      Esta información incluye el FQDN obligatorio de la máquina y se almacena en el archivo `certool.cfg`.
3. Si desea reemplazar el certificado raíz de Platform Services Controller en una implementación de varios nodos, siga estos pasos para cada nodo de vCenter Server.
   a. Reinicie los servicios en el nodo de vCenter Server.
   b. Regenere todos los certificados en la instancia de vCenter Servermediante las opciones 3 (`Replace Machine SSL certificate with VMCA Certificate`) y 6 (`Replace Solution user certificates with VMCA certificates`).

   Al reemplazar los certificados, VMCA firma con la cadena completa.

Pasos siguientes

Si desea realizar una actualización desde un entorno de vSphere 5.x, es posible que deba reemplazar el certificado de vCenter Single Sign-On dentro de vmdir. Consulte Reemplazar el certificado de VMware Directory Service en entornos de modo mixto.

Reemplazar un certificado SSL de máquina por un certificado de VMCA (entidad de certificación intermedia)

En una implementación de varios nodos donde se utiliza VMCA como entidad de certificación intermedia, es necesario reemplazar de forma explícita el certificado SSL de máquina. Primero, se debe reemplazar el certificado raíz de VMCA en el nodo de Platform Services Controller y, a continuación, se pueden reemplazar los certificados en los nodos de vCenter Server para tener la firma de la cadena completa en los certificados. También se puede utilizar esta opción para reemplazar certificados SSL de máquina que se encuentren dañados o a punto de caducar.

Al reemplazar el certificado SSL de máquina existente por un nuevo certificado firmado por VMCA, vSphere Certificate Manager solicita información e introduce todos los valores, excepto la contraseña y la dirección IP de Platform Services Controller, en el archivo `certool.cfg`.

- Contraseña de administrator@vsphere.local.
- Código de país de dos letras
- Nombre de empresa
- Nombre de organización
- Unidad de organización
- Estado
- Localidad
- Dirección IP (opcional)
- Correo electrónico
- Nombre del host, es decir, el nombre de dominio completo de la máquina para la que se desea reemplazar el certificado. Si el nombre del host no coincide con el FQDN, el reemplazo de los certificados no se completa correctamente y el entorno puede quedar en un estado inestable.
- Dirección IP de Platform Services Controller si ejecuta el comando en un nodo de administración.
- Nombre de VMCA, es decir, el nombre de dominio completo de la máquina en la que se ejecuta la configuración del certificado.

Requisitos previos

- Si reemplazó el certificado raíz de VMCA en una implementación de varios nodos, reinicie de forma explícita todos los nodos de vCenter Server.
- Para ejecutar Certificate Manager con esta opción, se necesita la siguiente información.
  - Contraseña de administrator@vsphere.local.
  - FQDN de la máquina para la cual se desea generar un nuevo certificado firmado por VMCA. Las demás propiedades tienen los valores predeterminados, pero pueden cambiarse.
  - Nombre de host o dirección IP de Platform Services Controller si se ejecuta en un sistema vCenter Server con una instancia de Platform Services Controller externa.

Procedimiento

1. Inicie vSphere Certificate Manager y seleccione la opción 3.
2. Responda las solicitudes del sistema.

   Certificate Manager almacenará la información en el archivo `certool.cfg`.

Resultados

vSphere Certificate Manager reemplazará el certificado SSL de máquina.

Reemplazar certificados de usuario de solución por certificados de VMCA (entidad de certificación intermedia)

En un entorno de varios nodos donde se utiliza VMCA como entidad de certificación intermedia, es posible reemplazar de forma explícita los certificados de usuario de solución. Primero, se debe reemplazar el certificado raíz de VMCA en el nodo de Platform Services Controller y, a continuación, se pueden reemplazar los certificados en los nodos de vCenter Server para tener la firma de la cadena completa en los certificados. También se puede utilizar esta opción para reemplazar certificados de usuario de solución que se encuentren dañados o a punto de caducar.

Requisitos previos

- Si reemplazó el certificado raíz de VMCA en una implementación de varios nodos, reinicie de forma explícita todos los nodos de vCenter Server.
- Para ejecutar Certificate Manager con esta opción, se necesita la siguiente información.
  - Contraseña de administrator@vsphere.local.
  - Nombre de host o dirección IP de Platform Services Controller si se ejecuta en un sistema vCenter Server con una instancia de Platform Services Controller externa.

Procedimiento

1. Inicie vSphere Certificate Manager y seleccione la opción 6.
2. Responda las solicitudes del sistema.

   Consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2112281 para obtener más información.

Resultados

vSphere Certificate Manager reemplazará todos los certificados de usuario de solución.

Reemplazar todos los certificados por certificados personalizados (Certificate Manager)

Es posible usar la utilidad vSphere Certificate Manager para reemplazar todos los certificados por certificados personalizados. Antes de iniciar el proceso, es necesario enviar solicitudes de firma de certificado (CSR) a la entidad de certificación. Se puede utilizar Certificate Manager para generar las CSR.

Una opción es reemplazar solo los certificados SSL de máquina y utilizar los certificados de usuario de solución que proporciona VMCA. Los certificados de usuario de solución se utilizan únicamente para la comunicación entre los componentes de vSphere.

Cuando se utilizan certificados personalizados, se deben reemplazar los certificados firmados por VMCA por certificados personalizados. Es posible utilizar vSphere Client, la utilidad vSphere Certificate Manager o las interfaces CLI para reemplazar manualmente los certificados. Los certificados se almacenarán en VECS.

Para reemplazar todos los certificados por certificados personalizados, debe ejecutar Certificate Manager varias veces. El flujo de trabajo ofrece el conjunto completo de pasos para reemplazar los certificados SSL de máquina y los certificados de usuarios de soluciones. Explica qué hacer en entornos con instancias integradas de Platform Services Controller o instancias externas de Platform Services Controller.

1 Se generan solicitudes de firma del certificado para el certificado SSL de máquina y los certificados de usuarios de soluciones por separado en cada equipo.

   a Para generar CSR del certificado SSL de máquina, seleccione la opción 1.

   b Si una directiva de la empresa no permite utilizar una implementación híbrida, se debe seleccionar la opción 5.

2 Después de recibir los certificados firmados y el certificado raíz de la CA, debe reemplazar el certificado SSL en cada equipo con la opción 1.

3 Si además desea reemplazar los certificados de usuarios de soluciones, seleccione la opción 5.

4 Por último, en una implementación de varios nodos, debe repetir el proceso en cada nodo.

Procedimiento

1 Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados)

   Es posible utilizar vSphere Certificate Manager para generar solicitudes de firma de certificado (CSR) y, a continuación, enviarlas a la entidad de certificación empresarial o a una entidad de certificación externa. Los certificados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

2 Reemplazar un certificado SSL de máquina por un certificado personalizado

   El certificado SSL de máquina se utiliza en el servicio de proxy inverso de cada nodo de administración, en Platform Services Controller y en la implementación integrada. Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. Puede reemplazar el certificado de cada nodo por un certificado personalizado.

3 Reemplazar los certificados de usuarios de soluciones con certificados personalizados

   Muchas empresas solo requieren que reemplace los certificados de los servicios a los que se puede acceder externamente. Sin embargo, Certificate Manager también permite reemplazar certificados de usuarios de solución. Los usuarios de la solución son colecciones de servicios, por ejemplo, todos los servicios asociados con vSphere Client. En las implementaciones de varios nodos, reemplace el certificado de usuario de la solución de máquina en Platform Services Controller y el conjunto completo de usuarios de solución en cada nodo de administración.

Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados)

Es posible utilizar vSphere Certificate Manager para generar solicitudes de firma de certificado (CSR) y, a continuación, enviarlas a la entidad de certificación empresarial o a una entidad de certificación externa. Los certificados se pueden utilizar en los diversos procesos de reemplazo de certificados compatibles.

Puede ejecutar la herramienta Certificate Manager en la línea de comandos de la siguiente manera:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Requisitos previos

vSphere Certificate Manager solicita información. La solicitud depende del entorno y del tipo de certificado que se desea reemplazar.

- Para cualquier tipo de generación de CSR, se solicita la contraseña del usuario administrator@vsphere.local o el administrador del dominio de vCenter Single Sign-On con el que se desea establecer la conexión.
- Cuando se desea generar una CSR en un entorno con una instancia externa de Platform Services Controller, se solicita el nombre de host o la dirección IP de Platform Services Controller.
- Para generar una CSR para un certificado SSL de máquina, se solicitan las propiedades del certificado, que están almacenadas en el archivo `certool.cfg`. En la mayoría de los campos, se puede aceptar el valor predeterminado o proporcionar valores específicos del sitio. Se requiere el FQDN de la máquina.

Procedimiento

1. En cada máquina del entorno, inicie vSphere Certificate Manager y seleccione la opción 1.
2. Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.
3. Seleccione la opción 1 para generar la CSR, responda las solicitudes del sistema y salga de Certificate Manager.

   Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.
4. Si también desea reemplazar todos los certificados de usuario de solución, reinicie Certificate Manager.

5 Seleccione la opción 5.

6 Si el sistema lo solicita, proporcione la contraseña y la dirección IP o el nombre de host de Platform Services Controller.

7 Seleccione la opción 1 para generar las CSR, responda las solicitudes del sistema y salga de Certificate Manager.

 Es necesario especificar un directorio como parte de este proceso. Certificate Manager colocará el certificado y los archivos de claves en el directorio.

 En cada nodo de Platform Services Controller, Certificate Manager generará un certificado y un par de claves. En cada nodo de vCenter Server, Certificate Manager generará cuatro certificados y pares de claves.

Pasos siguientes

Realice el reemplazo de certificados.

Reemplazar un certificado SSL de máquina por un certificado personalizado

El certificado SSL de máquina se utiliza en el servicio de proxy inverso de cada nodo de administración, en Platform Services Controller y en la implementación integrada. Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. Puede reemplazar el certificado de cada nodo por un certificado personalizado.

Requisitos previos

Antes de comenzar, se necesita una CSR para cada máquina del entorno. La CSR se puede generar mediante vSphere Certificate Manager o de forma explícita.

1 Para generar la CSR mediante vSphere Certificate Manager, consulte Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados).

2 Para generar la CSR de forma explícita, solicite un certificado para cada máquina a la entidad de certificación empresarial o externa. El certificado debe cumplir con los siguientes requisitos:

 - Tamaño de clave: 2.048 bits o más (formato codificado PEM)
 - Formato CRT
 - x509 versión 3
 - SubjectAltName debe contener DNS Name=<machine_FQDN>.
 - Contiene los siguientes usos de claves: firma digital, cifrado de clave

Nota No utilice los puntos de distribución de CRL, el acceso a la información de autoridad o la información de la plantilla de certificado en ningún certificado personalizado.

Consulte también el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2112014, Obtener certificados de vSphere de una entidad de certificación de Microsoft.

Procedimiento

1 Inicie vSphere Certificate Manager y seleccione la opción 1.

2 Seleccione la opción 2 para iniciar el reemplazo de certificados y responder a las solicitudes.

   vSphere Certificate Manager solicita la siguiente información:

   - Contraseña de administrator@vsphere.local.
   - Un certificado SSL de máquina personalizado y válido (archivo `.crt`).
   - Una clave SSL de máquina personalizada y válida (archivo `.key`).
   - Un certificado de firma válido para el certificado SSL de máquina personalizado (archivo `.crt`).
   - La dirección IP de Platform Services Controller si el comando se ejecuta en un nodo de administración dentro de una implementación de varios nodos.

Pasos siguientes

Si desea realizar una actualización desde un entorno de vSphere 5.x, deberá reemplazar el certificado de vCenter Single Sign-On en `vmdir`. Consulte Reemplazar el certificado de VMware Directory Service en entornos de modo mixto.

Reemplazar los certificados de usuarios de soluciones con certificados personalizados

Muchas empresas solo requieren que reemplace los certificados de los servicios a los que se puede acceder externamente. Sin embargo, Certificate Manager también permite reemplazar certificados de usuarios de solución. Los usuarios de la solución son colecciones de servicios, por ejemplo, todos los servicios asociados con vSphere Client. En las implementaciones de varios nodos, reemplace el certificado de usuario de la solución de máquina en Platform Services Controller y el conjunto completo de usuarios de solución en cada nodo de administración.

Cuando se le solicite un certificado de usuario de solución, proporcione la cadena de certificados de firma completa de la entidad de certificación externa.

El formato debe ser similar al siguiente mensaje.

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

Requisitos previos

Antes de comenzar, se necesita una CSR para cada máquina del entorno. La CSR se puede generar mediante vSphere Certificate Manager o de forma explícita.

1 Para generar la CSR mediante vSphere Certificate Manager, consulte Generar solicitudes de firma de certificado con vSphere Certificate Manager (certificados personalizados).

2 Solicite un certificado para cada usuario de solución en cada nodo a la CA empresarial o externa. Puede generar la CSR mediante vSphere Certificate Manager o prepararla usted mismo. La CSR debe cumplir con los siguientes requisitos:

   - Tamaño de clave: 2.048 bits o más (formato codificado PEM)
   - Formato CRT
   - x509 versión 3
   - SubjectAltName debe contener DNS Name=<machine_FQDN>.
   - Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como vpxd) u otro identificador único.
   - Contiene los siguientes usos de claves: firma digital, cifrado de clave

Consulte también el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2112014, Obtener certificados de vSphere de una entidad de certificación de Microsoft.

Procedimiento

1 Inicie vSphere Certificate Manager y seleccione la opción 5.

2 Seleccione la opción 2 para iniciar el reemplazo de certificados y responder a las solicitudes.

   vSphere Certificate Manager solicita la siguiente información:

   - Contraseña de administrator@vsphere.local.
   - Certificado y clave del usuario de solución de la máquina.
   - Si se ejecuta vSphere Certificate Manager en un nodo de Platform Services Controller, se solicita el certificado y la clave (`vpxd.crt` y `vpxd.key`) del usuario de solución de la máquina.
   - Si se ejecuta vSphere Certificate Manager en un nodo de administración o en una implementación integrada, se solicita el conjunto completo de certificados y claves (`vpxd.crt` y `vpxd.key`) de todos los usuarios de solución.

Pasos siguientes

Si desea realizar una actualización desde un entorno de vSphere 5.x, es posible que deba reemplazar el certificado de vCenter Single Sign-On dentro de vmdir. Consulte Reemplazar el certificado de VMware Directory Service en entornos de modo mixto.

Revertir la última operación realizada volviendo a publicar certificados antiguos

Cuando se realiza una operación de administración de certificados mediante vSphere Certificate Manager, primero se almacena el estado actual del certificado en BACKUP_STORE, en VECS, antes del reemplazo de los certificados. Es posible revertir la última operación realizada y regresar al estado anterior.

Nota La operación de reversión restablece lo que actualmente se encuentra en BACKUP_STORE. Si ejecuta vSphere Certificate Manager con dos opciones diferentes y, a continuación, intenta hacer la reversión, solo se revierte la última operación.

Restablecer todos los certificados

Puede usar la opción `Reset All Certificates` (Restablecer todos los certificados) para reemplazar los certificados de vCenter existentes por los certificados firmados por VMCA.

Cuando utiliza esta opción, se sobrescriben todos los certificados personalizados que actualmente figuran en VECS.

- En un nodo de Platform Services Controller, vSphere Certificate Manager puede volver a generar el certificado raíz, y reemplazar el certificado SSL de máquina y el certificado del usuario de solución de la máquina.
- En un nodo de administración, vSphere Certificate Manager puede reemplazar el certificado SSL de máquina y todos los certificados de los usuarios de solución.
- En una implementación integrada, vSphere Certificate Manager puede reemplazar todos los certificados.

Qué certificados se reemplacen dependerá de las opciones que se seleccionen.

Reemplazar certificados de forma manual

En algunos casos especiales, por ejemplo, si desea reemplazar solo un tipo de certificado de usuario de solución, no puede utilizar la utilidad vSphere Certificate Manager. En ese caso, puede usar las CLI incluidas en la instalación para el reemplazo de certificados.

Información sobre la interrupción y el inicio de servicios

Para determinadas partes del reemplazo manual de certificados, se deben detener todos los servicios y, a continuación, iniciar únicamente los servicios que administran la infraestructura de certificados. Al detener los servicios solo cuando es necesario, se reduce el tiempo de inactividad.

Como parte del proceso de reemplazo de certificados, es necesario detener e iniciar los servicios. Puede usar el comando `service-control` para iniciar y detener servicios. Puede iniciar y detener todos los servicios o servicios individuales. Consulte la ayuda de la línea de comandos para obtener más información.

- Si el entorno utiliza una instancia integrada de Platform Services Controller, debe iniciar y detener todos los servicios, tal como se describe en este documento.
- Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Dichos servicios se ejecutan en Platform Services Controller.

Siga estas directrices.

- No detenga los servicios para generar nuevos pares de claves públicas/privadas o nuevos certificados.
- Si es el único administrador, no es necesario que detenga los servicios al agregar un nuevo certificado raíz. El certificado raíz anterior sigue disponible y todos los servicios pueden seguir autenticándose con ese certificado. Una vez que se haya agregado el certificado raíz, detenga y reinicie de inmediato todos los servicios para evitar problemas con los hosts.
- Si el entorno incluye varios administradores, detenga los servicios antes de agregar un nuevo certificado raíz y reinícielos una vez que se haya agregado el nuevo certificado.
- Detenga los servicios justo antes de realizar estas tareas:
  - Eliminar un certificado SSL de máquina o cualquier certificado de usuario de solución en VECS.
  - Reemplazar un certificado de usuario de solución en vmdir (VMware Directory Service).

Reemplazar certificados firmados por VMCA existentes por certificados firmados por VMCA nuevos

Si el certificado raíz de VMCA está por caducar, o si desea reemplazarlo por otros motivos, puede generar un certificado raíz nuevo y agregarlo a VMware Directory Service. A continuación, puede generar certificados SSL de máquina y certificados de usuarios de solución nuevos mediante el certificado raíz nuevo.

Use la utilidad vSphere Certificate Manager para reemplazar certificados en la mayoría de los casos.

Si necesita tener un control detallado, este caso ofrece instrucciones detalladas paso a paso para reemplazar el conjunto completo de certificados mediante comandos de CLI. O bien puede reemplazar certificados individuales mediante el procedimiento de la tarea correspondiente.

Requisitos previos

Solo administrator@vsphere.local u otros usuarios del grupo Administradores de CA pueden realizar tareas de administración de certificados. Consulte Agregar miembros a un grupo de vCenter Single Sign-On.

Procedimiento

1 Generar un nuevo certificado raíz firmado por VMCA

Genere nuevos certificados firmados por VMCA con la CLI `certool` o la utilidad de vSphere Certificate Manager, y publique los certificados en vmdir.

2 Reemplazar certificados SSL de máquina por certificados firmados por VMCA

Después de generar un nuevo certificado raíz firmado por VMCA, puede reemplazar todos los certificados SSL de máquina en el entorno.

3 Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA

Después de reemplazar los certificados SSL de máquina, puede reemplazar todos los certificados de usuarios de solución. Los certificados de usuario de solución deben ser válidos, es decir, que no estén caducados, pero la infraestructura de certificados no utiliza ninguna otra información del certificado.

4 Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

Generar un nuevo certificado raíz firmado por VMCA

Genere nuevos certificados firmados por VMCA con la CLI `certool` o la utilidad de vSphere Certificate Manager, y publique los certificados en vmdir.

En una implementación de varios nodos, los comandos para generar certificados raíz se ejecutan en Platform Services Controller.

Procedimiento

1 Genere un nuevo certificado autofirmado y una clave privada.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 Reemplace el certificado raíz existente con el nuevo certificado.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

El comando genera el certificado, lo agrega a vmdir y, a continuación, lo agrega a VECS.

3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 (opcional) Publique el nuevo certificado raíz en vmdir.

```
dir-cli trustedcert publish --cert newRoot.crt
```

El comando actualiza todas las instancias de vmdir de manera inmediata. Si no lo ejecuta, la propagación del nuevo certificado a todos los nodos puede tardar un poco.

5 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Generar un nuevo certificado raíz firmado por VMCA

El siguiente ejemplo muestra todos los pasos para comprobar la información de la entidad de certificación raíz actual y volver a generar el certificado raíz.

1 (Opcional) Enumere el certificado raíz de VMCA para asegurarse de que se encuentre en el almacén de certificados.

- En una instalación integrada o un nodo de Platform Services Controller:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- En un nodo de administración (instalación externa):

  ```
  C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-ip-or-fqdn>
  ```

La salida se parece a esto:

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 (Opcional) Enumere el almacén TRUSTED_ROOTS de VECS y compare el número de serie del certificado con la salida del paso 1.

Este comando funciona tanto en nodos de Platform Services Controller como de administración, ya que VECS sondea vmdir.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS
--text
```

En el caso más simple con un solo certificado raíz, la salida se parece a esto:

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
```

3 Genere un nuevo certificado raíz de VMCA. El comando agrega el certificado al almacén TRUSTED_ROOTS en VECS y en vmdir (VMware Directory Service).

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

En Windows, `--config` es opcional porque el comando usa el archivo predeterminado `certool.cfg`.

Reemplazar certificados SSL de máquina por certificados firmados por VMCA

Después de generar un nuevo certificado raíz firmado por VMCA, puede reemplazar todos los certificados SSL de máquina en el entorno.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. En una implementación de varios nodos, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo. Use el parámetro `--server` para apuntar a Platform Services Controller desde vCenter Server con Platform Services Controller externo.

Requisitos previos

Prepárese para detener todos los servicios y para iniciar los servicios que controlan la propagación y el almacenamiento de certificados.

Procedimiento

1 Haga una copia de `certool.cfg` para cada máquina que necesite un certificado nuevo.

Puede encontrar `certool.cfg` en las siguientes ubicaciones:

Sistema operativo	Ruta de acceso
Windows	`C:\Archivos de programa\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

2 Edite el archivo de configuración personalizado de cada máquina a fin de incluir el FQDN de la máquina.

Ejecute `NSLookup` sobre la dirección IP de la máquina a fin de ver el listado de DNS del nombre y usar ese nombre en el campo Nombre de host del archivo.

3 Genere un par de archivos de clave pública/privada y un certificado para cada archivo pasando el archivo de configuración que acaba de personalizar.

Por ejemplo:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Agregue el certificado nuevo a VECS.

Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL. Primero debe eliminar la entrada existente y, a continuación, agregar la nueva.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.crt
 --key machine1.priv
```

6 Reinicie todos los servicios.

```

service-control --start --all
```

Ejemplo: Reemplazo de certificados de una máquina por certificados firmados por VMCA

1 Cree un archivo de configuración para el certificado SSL y guárdelo como `ssl-config.cfg` en el directorio actual.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 Genere un par de claves para el certificado SSL de máquina. Ejecute este comando en cada nodo de administración y en el nodo de Platform Services Controller. No se requiere la opción `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Los archivos `ssl-key.priv` y `ssl-key.pub` se crean en el directorio actual.

3 Genere el nuevo certificado SSL de máquina. Este certificado está firmado por VMCA. Si reemplazó el certificado raíz de VMCA por un certificado personalizado, VMCA firma todos los certificados con la cadena completa.

- En una instalación integrada o un nodo de Platform Services Controller:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- En vCenter Server (instalación externa):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

El archivo `new-vmca-ssl.crt` se crea en el directorio actual.

4 (Opcional) Enumere el contenido de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Ejemplo de salida en Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Ejemplo de salida en vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 Reemplace el certificado SSL de máquina en VECS por el nuevo certificado SSL de máquina. Los valores `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados.

- En Platform Services Controller, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE_SSL_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- En cada nodo de administración o en la implementación integrada, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE_SSL_CERT. Debe actualizar el certificado para cada máquina por separado, ya que cada una de ellas tiene un FQDN diferente.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Pasos siguientes

También puede reemplazar los certificados de sus hosts ESXi. Consulte la publicación *Seguridad de vSphere*.

Después de reemplazar el certificado raíz en una implementación de varios nodos, debe reiniciar los servicios en todas las instancias de vCenter Server con nodos de Platform Services Controller externo.

Reemplazar los certificados de usuario de solución por certificados nuevos firmados por VMCA

Después de reemplazar los certificados SSL de máquina, puede reemplazar todos los certificados de usuarios de solución. Los certificados de usuario de solución deben ser válidos, es decir, que no estén caducados, pero la infraestructura de certificados no utiliza ninguna otra información del certificado.

Muchos clientes de VMware no reemplazan los certificados de usuario de las soluciones. Reemplazan solo los certificados SSL de los equipos con certificados personalizados. Este enfoque híbrido satisface los requisitos de sus equipos de seguridad.

- Los certificados se sientan detrás de un proxy, o bien son certificados personalizados.
- No se utilizan CA intermedias.

Debe reemplazar el certificado de usuario de solución de la máquina en cada nodo de administración y en cada nodo de Platform Services Controller. Debe reemplazar los certificados de usuarios de solución solo en cada nodo de administración. Utilice el parámetro `--server` para apuntar a Platform Services Controller cuando ejecute comandos en un nodo de administración con una instancia externa de Platform Services Controller.

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

Requisitos previos

Prepárese para detener todos los servicios y para iniciar los servicios que controlan la propagación y el almacenamiento de certificados.

Procedimiento

1 Haga una copia de `certool.cfg`, quite los campos Nombre, Dirección IP, Correo electrónico y Nombre DNS, y cambie el nombre del archivo: por ejemplo, a `sol_usr.cfg`.

   Se pueden nombrar los certificados desde la línea de comandos como parte de la generación. La otra información no es necesaria para los usuarios de solución. Si se deja la información predeterminada, los certificados generados podrían resultar confusos.

2 Genere un par de archivos de clave pública/privada y un certificado para cada usuario de solución y pase el archivo de configuración que recién personalizó.

   Por ejemplo:

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 Busque el nombre de cada usuario de solución.

```
dir-cli service list
```

   Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Cuando enumera certificados de usuario de solución en implementaciones de varios nodos, el resultado de la lista de `dir-cli` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 En cada usuario de solución, reemplace el certificado actual en vmdir y, a continuación, en VECS.

El siguiente ejemplo muestra cómo reemplazar los certificados del servicio vpxd.

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Nota Los usuarios de solución no podrán autenticarse en vCenter Single Sign-On si no se reemplaza el certificado en vmdir.

6 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Usar los certificados de usuarios de solución firmados por VMCA

1 Genere un par de claves pública/privada para cada usuario de solución. Esto incluye un par para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, y un par para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient) en cada nodo de administración.

   a Genere un par de claves para el usuario de solución de la máquina de una implementación integrada o para el usuario de solución de la máquina de Platform Services Controller.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   b (Opcional) Para implementaciones con una instancia de Platform Services Controller externa, genere un par de claves para el usuario de solución de la máquina en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   c Genere un par de claves para el usuario de solución vpxd en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
   ```

   d Genere un par de claves para el usuario de solución vpxd-extension en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
   ```

   e Genere un par de claves para el usuario de solución vsphere-webclient en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
   ```

2 Genere certificados de usuarios de solución que estén firmados con el nuevo certificado raíz de VMCA para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, así como para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient) en cada nodo de administración.

Nota El parámetro `--Name` tiene que ser único. Al incluir el nombre del almacén del usuario de solución, resulta más fácil ver qué certificado se asigna a cada usuario de solución. El ejemplo incluye el nombre, por ejemplo, `vpxd` o `vpxd-extension` en cada caso.

a Ejecute el siguiente comando en el nodo de Platform Services Controller a fin de generar un certificado de usuario de solución de la máquina en ese nodo.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
machine.crt --privkey=machine-key.priv --Name=machine
```

b Genere un certificado para el usuario de solución de la máquina en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c Genere un certificado para el usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d Genere un certificado para el usuario de solución vpxd-extensions en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-
extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-
or-fqdn>
```

e Ejecute el siguiente comando para generar un certificado para el usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --
server=<psc-ip-or-fqdn>
```

3 Reemplace los certificados de usuario de solución en VECS por los nuevos certificados de usuario de solución.

Nota Los parámetros `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados de los servicios.

a En el nodo de Platform Services Controller, ejecute el siguiente comando para reemplazar el certificado de usuario de solución de la máquina.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b Reemplace el certificado de usuario de solución de la máquina en cada nodo de administración:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Reemplace el certificado de usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d Reemplace el certificado de usuario de solución vpxd-extension en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

e Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 Actualice VMware Directory Service (vmdir) con los nuevos certificados de usuarios de solución. Se solicita una contraseña de administrador de vCenter Single Sign-On.

   a Ejecute `dir-cli service list` para obtener el sufijo de identificador único de servicio para cada usuario de solución. Puede ejecutar este comando en un sistema Platform Services Controller o vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

   b Reemplace el certificado de máquina en vmdir de Platform Services Controller. Por ejemplo, si machine-29a45d00-60a7-11e4-96ff-00505689639a es el usuario de solución de la máquina en Platform Services Controller, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

   c Reemplace el certificado de la máquina en vmdir en cada nodo de administración. Por ejemplo, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 es el usuario de solución de la máquina en vCenter Server, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

   d Reemplace el certificado de usuario de solución vpxd en vmdir en cada nodo de administración. Por ejemplo, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

   e Reemplace el certificado de usuario de solución vpxd-extension en vmdir en cada nodo de administración. Por ejemplo, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd-extension, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración. Por ejemplo, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vsphere-webclient, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Pasos siguientes

Reinicie todos los servicios de cada nodo de Platform Services Controller y cada nodo de administración.

Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

El vmdir utiliza el certificado SSL de VMware Directory Service para realizar negociaciones entre los nodos de Platform Services Controller que realizan la replicación de vCenter Single Sign-On.

Estos pasos no son necesarios para un entorno de modo mixto que incluya los nodos de vSphere 6.0 y vSphere 6.5. Estos pasos son necesarios solo si:

- El entorno incluye servicios tanto de vCenter Single Sign-On 5.5 como de vCenter Single Sign-On 6.x.
- Los servicios de vCenter Single Sign-On se configuran para replicar datos de vmdir.
- Planea reemplazar los certificados firmados por VMCA predeterminados por certificados personalizados del nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x.

Nota Actualizar el entorno al completo antes de reiniciar los servicios es una práctica recomendada. Generalmente, el reemplazo del certificado de VMware Directory Service no se recomienda.

Procedimiento

1 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 5.5, configure el entorno para que se reconozca el servicio de vCenter Single Sign-On 6.x.

   a Haga una copia de seguridad de todos los archivos C:\ProgramData\VMware\CIS\cfg\vmdird.

   b Haga una copia del archivo vmdircert.pem en el nodo 6.x y cámbiele el nombre por <sso_node2.domain.com>.pem, donde <sso_node2.domain.com> es el FQDN del nodo 6.x.

   c Copie el certificado con nombre nuevo en C:\ProgramData\VMware\CIS\cfg\vmdird para reemplazar el certificado de replicación existente.

2 Reinicie VMware Directory Service en todas las máquinas en las que reemplazó certificados.

   Puede reiniciar el servicio desde vSphere Client o utilizar el comando service-control.

Utilizar VMCA como entidad de certificación intermedia

Puede reemplazar el certificado raíz de VMCA por un certificado externo firmado por una entidad de certificación en la que se incluya VMCA en la cadena de certificados. Más adelante, todos los certificados generados por VMCA incluirán la cadena completa. Puede reemplazar los certificados existentes por certificados generados recientemente.

Procedimiento

1 Reemplazar el certificado raíz (entidad de certificación intermedia)

   El primer paso para reemplazar los certificados VMCA por certificados personalizados es generar una CSR mediante el envío de la CSR que se debe firmar. A continuación, el certificado firmado se agrega a VMCA como certificado raíz.

2 Reemplazar certificados SSL de máquina (entidad de certificación intermedia)

   Después de recibir el certificado firmado de la CA y convertirlo en el certificado raíz de VMCA, puede reemplazar todos los certificados SSL de máquina.

3 Reemplazar certificados de usuarios de solución (entidad de certificación intermedia)

   Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de los usuarios de solución.

4 Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

   Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

Reemplazar el certificado raíz (entidad de certificación intermedia)

El primer paso para reemplazar los certificados VMCA por certificados personalizados es generar una CSR mediante el envío de la CSR que se debe firmar. A continuación, el certificado firmado se agrega a VMCA como certificado raíz.

Se puede utilizar la utilidad Certificate Manager u otra herramienta para generar la CSR. La CSR debe cumplir con los siguientes requisitos:

- Tamaño de clave: 2.048 bits o más
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- Si utiliza certificados personalizados, la extensión CA debe establecerse con el valor true para certificados de raíz, y el signo cert debe estar en la lista de requisitos.
- La firma CRL debe estar habilitada.
- El uso mejorado de clave puede estar vacío o contener autenticación del servidor.
- No hay límite explícito a la longitud de la cadena de certificados. VMCA utiliza el valor predeterminado de OpenSSL, que es de diez certificados.
- No se admiten los certificados con comodines o con más de un nombre DNS.
- No se pueden crear CA subsidiarias de VMCA.

  Para obtener un ejemplo de uso de la entidad de certificación de Microsoft, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2112009, Crear una plantilla de entidad de certificación de Microsoft para creación de certificados SSL en vSphere 6.0.

VMCA valida los siguientes atributos de certificados al reemplazar el certificado raíz:

- Tamaño de clave de 2048 bits o más
- Uso de clave: firma de certificado
- Restricción básica: entidad de certificación de tipo sujeto

Procedimiento

1 Genere una CSR y envíela a la entidad de certificación.

  Siga las instrucciones de la entidad de certificación.

2 Prepare un archivo de certificado que incluya el certificado VMCA firmado y la cadena de entidad de certificación completa de la entidad de certificación empresarial o de terceros. Guarde el archivo, por ejemplo como `rootca1.crt`.

Para aplicar este paso, se pueden copiar todos los certificados de la entidad de certificación en formato PEM en un solo archivo. Comience con el certificado raíz VMCA y termine con el certificado raíz PEM de la entidad de certificación. Por ejemplo:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Reemplace la entidad de certificación raíz VMCA existente.

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

Al ejecutarse, este comando realiza lo siguiente:

- Agrega el nuevo certificado raíz personalizado a la ubicación de certificados en el sistema de archivos.

- Anexa el certificado raíz personalizado al almacén TRUSTED_ROOTS en VECS (después de una demora).
- Agrega el certificado raíz personalizado a vmdir (después de una demora).

5 (opcional) Para propagar el cambio a todas las instancias de vmdir (VMware Directory Service), publique el nuevo certificado raíz en vmdir suministrando la ruta de acceso para cada archivo.

   Por ejemplo:

```
dir-cli trustedcert publish --cert rootca1.crt
```

   Cada 30 segundos se produce la replicación entre los nodos de vmdir. No se necesita agregar el certificado raíz a VECS explícitamente, ya que VECS sondea vmdir cada 5 minutos en busca de nuevos archivos de certificados raíz.

6 (opcional) Si fuera necesario, se puede forzar la actualización de VECS.

```
vecs-cli force-refresh
```

7 Reinicie todos los servicios.

```

service-control --start --all
```

Ejemplo: Reemplazo del certificado raíz

Reemplace el certificado raíz de VMCA por el certificado raíz personalizado de la entidad de certificación mediante el comando certool con la opción `--rootca`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-
certs\root.pem --privkey=C:\custom-certs\root.key
```

Al ejecutarse, este comando realiza lo siguiente:

- Agrega el nuevo certificado raíz personalizado a la ubicación de certificados en el sistema de archivos.
- Anexa el certificado raíz personalizado al almacén TRUSTED_ROOTS en VECS.
- Agrega el certificado raíz personalizado a vmdir.

Pasos siguientes

Se puede eliminar el certificado raíz original de VMCA del almacén de certificados si así lo establece la directiva de la empresa. Si se hace eso, es necesario reemplazar el certificado de firma de vCenter Single Sign-On. Consulte Actualizar el certificado del servicio de token de seguridad.

Reemplazar certificados SSL de máquina (entidad de certificación intermedia)

Después de recibir el certificado firmado de la CA y convertirlo en el certificado raíz de VMCA, puede reemplazar todos los certificados SSL de máquina.

Estos pasos son prácticamente los mismos que los pasos para reemplazar un certificado por otro que utilice VMCA como entidad de certificación. Sin embargo, en este caso, VMCA firma todos los certificados con la cadena completa.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. En una implementación de varios nodos, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo. Use el parámetro `--server` para apuntar a Platform Services Controller desde vCenter Server con Platform Services Controller externo.

Requisitos previos

Para el certificado SSL de máquina, el `SubjectAltName` debe contener `DNS Name=<Machine FQDN>`.

Procedimiento

1 Haga una copia de `certool.cfg` para cada máquina que necesite un certificado nuevo.

   Puede encontrar `certool.cfg` en las siguientes ubicaciones:

   Windows

   `C:\Archivos de programa\VMware\vCenter Server\vmcad`

   Linux

   `/usr/lib/vmware-vmca/share/config/`

2 Edite el archivo de configuración personalizado de cada máquina a fin de incluir el FQDN de la máquina.

   Ejecute `NSLookup` sobre la dirección IP de la máquina a fin de ver el listado de DNS del nombre y usar ese nombre en el campo Nombre de host del archivo.

3 Genere un par de archivos de clave pública/privada y un certificado para cada máquina pasando el archivo de configuración que acaba de personalizar.

   Por ejemplo:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Agregue el certificado nuevo a VECS.

Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL. Primero debe eliminar la entrada existente y, a continuación, agregar la nueva.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 Reinicie todos los servicios.

```

service-control --start --all
```

Ejemplo: Reemplazo de certificados SSL de máquina (VMCA es la CA intermedia)

1 Cree un archivo de configuración para el certificado SSL y guárdelo como `ssl-config.cfg` en el directorio actual.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 Genere un par de claves para el certificado SSL de máquina. Ejecute este comando en cada nodo de administración y en el nodo de Platform Services Controller. No se requiere la opción `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Los archivos `ssl-key.priv` y `ssl-key.pub` se crean en el directorio actual.

3 Genere el nuevo certificado SSL de máquina. Este certificado está firmado por VMCA. Si reemplazó el certificado raíz de VMCA por un certificado personalizado, VMCA firma todos los certificados con la cadena completa.

- En una instalación integrada o un nodo de Platform Services Controller:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- En vCenter Server (instalación externa):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

El archivo `new-vmca-ssl.crt` se crea en el directorio actual.

4 (Opcional) Enumere el contenido de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Ejemplo de salida en Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Ejemplo de salida en vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 Reemplace el certificado SSL de máquina en VECS por el nuevo certificado SSL de máquina. Los valores `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados.

- En Platform Services Controller, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE_SSL_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- En cada nodo de administración o en la implementación integrada, ejecute el siguiente comando para actualizar el certificado SSL de máquina en el almacén MACHINE_SSL_CERT. Debe actualizar el certificado para cada máquina por separado, ya que cada una de ellas tiene un FQDN diferente.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Reemplazar certificados de usuarios de solución (entidad de certificación intermedia)

Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de los usuarios de solución.

Muchos clientes de VMware no reemplazan los certificados de usuario de las soluciones. Reemplazan solo los certificados SSL de los equipos con certificados personalizados. Este enfoque híbrido satisface los requisitos de sus equipos de seguridad.

- Los certificados se sientan detrás de un proxy, o bien son certificados personalizados.
- No se utilizan CA intermedias.

Debe reemplazar el certificado de usuario de solución de la máquina en cada nodo de administración y en cada nodo de Platform Services Controller. Debe reemplazar los certificados de usuarios de solución solo en cada nodo de administración. Utilice el parámetro `--server` para apuntar a Platform Services Controller cuando ejecute comandos en un nodo de administración con una instancia externa de Platform Services Controller.

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

Requisitos previos

Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como vpxd) u otro identificador único.

Nota El almacén de certificados de vpxd existe solo en el vCenter Server Appliance, no en el Platform Services Controller.

Procedimiento

1 Haga una copia de `certool.cfg`, quite los campos Nombre, Dirección IP, Correo electrónico y Nombre DNS, y cambie el nombre del archivo: por ejemplo, a `sol_usr.cfg`.

   Se pueden nombrar los certificados desde la línea de comandos como parte de la generación. La otra información no es necesaria para los usuarios de solución. Si se deja la información predeterminada, los certificados generados podrían resultar confusos.

2 Genere un par de archivos de clave pública/privada y un certificado para cada usuario de solución y pase el archivo de configuración que recién personalizó.

   Por ejemplo:

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 Busque el nombre de cada usuario de solución.

```
dir-cli service list
```

   Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

   Cuando enumera certificados de usuario de solución en implementaciones de varios nodos, el resultado de la lista de `dir-cli` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

4 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Reemplace el certificado que ya existe primero en vmdir y después en VECS.

Debe agregar los certificados en ese orden para los usuarios de solución. Por ejemplo:

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Nota Los usuarios de solución no pueden iniciar sesión en vCenter Single Sign-On si no reemplaza el certificado en vmdir.

6 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Reemplazo de certificados de usuarios de solución (entidad de certificación intermedia)

1 Genere un par de claves pública/privada para cada usuario de solución. Esto incluye un par para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, y un par para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient) en cada nodo de administración.

   a Genere un par de claves para el usuario de solución de la máquina de una implementación integrada o para el usuario de solución de la máquina de Platform Services Controller.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   b (Opcional) Para implementaciones con una instancia de Platform Services Controller externa, genere un par de claves para el usuario de solución de la máquina en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   c Genere un par de claves para el usuario de solución vpxd en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
   ```

   d Genere un par de claves para el usuario de solución vpxd-extension en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
   ```

   e Genere un par de claves para el usuario de solución vsphere-webclient en cada nodo de administración.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
   ```

2 Genere certificados de usuarios de solución que estén firmados con el nuevo certificado raíz de VMCA para el usuario de solución de la máquina en cada instancia de Platform Services Controller y en cada nodo de administración, así como para cada usuario de solución adicional (vpxd, vpxd-extension, vsphere-webclient) en cada nodo de administración.

Nota El parámetro `--Name` tiene que ser único. Al incluir el nombre del almacén del usuario de solución, resulta más fácil ver qué certificado se asigna a cada usuario de solución. El ejemplo incluye el nombre, por ejemplo, `vpxd` o `vpxd-extension` en cada caso.

a Ejecute el siguiente comando en el nodo de Platform Services Controller a fin de generar un certificado de usuario de solución de la máquina en ese nodo.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

b Genere un certificado para el usuario de solución de la máquina en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c Genere un certificado para el usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d Genere un certificado para el usuario de solución vpxd-extensions en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

e Ejecute el siguiente comando para generar un certificado para el usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

3 Reemplace los certificados de usuario de solución en VECS por los nuevos certificados de usuario de solución.

Nota Los parámetros `--store` y `--alias` tienen que coincidir exactamente con los nombres predeterminados de los servicios.

---

a En el nodo de Platform Services Controller, ejecute el siguiente comando para reemplazar el certificado de usuario de solución de la máquina.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b Reemplace el certificado de usuario de solución de la máquina en cada nodo de administración:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Reemplace el certificado de usuario de solución vpxd en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d Reemplace el certificado de usuario de solución vpxd-extension en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

e Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 Actualice VMware Directory Service (vmdir) con los nuevos certificados de usuarios de solución. Se solicita una contraseña de administrador de vCenter Single Sign-On.

a Ejecute `dir-cli service list` para obtener el sufijo de identificador único de servicio para cada usuario de solución. Puede ejecutar este comando en un sistema Platform Services Controller o vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

b Reemplace el certificado de máquina en vmdir de Platform Services Controller. Por ejemplo, si machine-29a45d00-60a7-11e4-96ff-00505689639a es el usuario de solución de la máquina en Platform Services Controller, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c Reemplace el certificado de la máquina en vmdir en cada nodo de administración. Por ejemplo, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 es el usuario de solución de la máquina en vCenter Server, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d Reemplace el certificado de usuario de solución vpxd en vmdir en cada nodo de administración. Por ejemplo, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e Reemplace el certificado de usuario de solución vpxd-extension en vmdir en cada nodo de administración. Por ejemplo, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vpxd-extension, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f Reemplace el certificado de usuario de solución vsphere-webclient en cada nodo de administración. Por ejemplo, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 es el identificador de usuario de solución vsphere-webclient, ejecute este comando:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

El vmdir utiliza el certificado SSL de VMware Directory Service para realizar negociaciones entre los nodos de Platform Services Controller que realizan la replicación de vCenter Single Sign-On.

Estos pasos no son necesarios para un entorno de modo mixto que incluya los nodos de vSphere 6.0 y vSphere 6.5. Estos pasos son necesarios solo si:

- El entorno incluye servicios tanto de vCenter Single Sign-On 5.5 como de vCenter Single Sign-On 6.x.
- Los servicios de vCenter Single Sign-On se configuran para replicar datos de vmdir.
- Planea reemplazar los certificados firmados por VMCA predeterminados por certificados personalizados del nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x.

Nota Actualizar el entorno al completo antes de reiniciar los servicios es una práctica recomendada. Generalmente, el reemplazo del certificado de VMware Directory Service no se recomienda.

Procedimiento

1 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 5.5, configure el entorno para que se reconozca el servicio de vCenter Single Sign-On 6.x.

a Haga una copia de seguridad de todos los archivos `C:\ProgramData\VMware\CIS\cfg\vmdird`.

b Haga una copia del archivo `vmdircert.pem` en el nodo 6.x y cámbiele el nombre por `<sso_node2.domain.com>.pem`, donde `<sso_node2.domain.com>` es el FQDN del nodo 6.x.

c Copie el certificado con nombre nuevo en `C:\ProgramData\VMware\CIS\cfg\vmdird` para reemplazar el certificado de replicación existente.

2 Reinicie VMware Directory Service en todas las máquinas en las que reemplazó certificados.

Puede reiniciar el servicio desde vSphere Client o utilizar el comando `service-control`.

Usar certificados personalizados con vSphere

Si la directiva de la empresa lo requiere, puede reemplazar de manera total o parcial los certificados utilizados en vSphere por certificados firmados por una CA de la empresa o externa. Si lo hace, VMCA no estará en la cadena de certificados. Es su responsabilidad almacenar todos los certificados de vCenter en VECS.

Puede reemplazar todos los certificados o utilizar una solución híbrida. Por ejemplo, considere reemplazar todos los certificados que se utilizan para el tráfico de red y dejar los certificados de usuarios de solución firmados por VMCA. Los certificados de usuarios de solución se utilizan solo para efectuar la autenticación en vCenter Single Sign-On.

Nota Si no desea utilizar VMCA, es su responsabilidad reemplazar todos los certificados, aprovisionar componentes nuevos con certificados y hacer un seguimiento de la caducidad de los certificados.

Incluso si decide utilizar certificados personalizados, puede continuar usando la utilidad de VMware Certificate Manager para reemplazar los certificados. Consulte Reemplazar todos los certificados por certificados personalizados (Certificate Manager).

Si tiene problemas con vSphere Auto Deploy después de reemplazar los certificados, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2000988.

Procedimiento

1 Solicitar certificados e importar un certificado raíz personalizado

   Puede utilizar certificados personalizados de una CA de la empresa o externa. El primer paso es solicitar los certificados a la entidad de certificación e importar los certificados raíz en VMware Endpoint Certificate Store (VECS).

2 Reemplazar certificados SSL de máquina por certificados personalizados

   Después de recibir los certificados personalizados, puede reemplazar los certificados de cada máquina.

3 Reemplazar los certificados de usuarios de soluciones con certificados personalizados

   Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de usuarios de solución firmados por VMCA con certificados externas o empresariales.

4 Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

   Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

Solicitar certificados e importar un certificado raíz personalizado

Puede utilizar certificados personalizados de una CA de la empresa o externa. El primer paso es solicitar los certificados a la entidad de certificación e importar los certificados raíz en VMware Endpoint Certificate Store (VECS).

Requisitos previos

El certificado debe cumplir con los siguientes requisitos:

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato PEM. VMware admite PKCS8 y PKCS1 (claves RSA). Cuando se agregan claves a VECS, se convierten en PKCS8.
- x509 versión 3
- Para los certificados raíz, la extensión CA se debe establecer en true y el signo cert debe estar en la lista de requisitos.
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Formato CRT
- Contiene los siguientes usos de claves: firma digital, cifrado de clave
- Hora de inicio de un día anterior a la hora actual.
- CN (y SubjectAltName) establecidos con el nombre de host (o dirección IP) que el host ESXi tiene en el inventario de vCenter Server.

Procedimiento

1 Envíe las solicitudes de firma de certificados (Certificate Signing Requests, CSR) para los siguientes certificados al proveedor de certificados de la empresa o externo.

   - Un certificado SSL de máquina para cada máquina. Para el certificado SSL de máquina, el campo SubjectAltName debe contener el nombre de dominio completo (DNS NAME=*FQDN_de_máquina*).
   - De forma opcional, cuatro certificados de usuario de solución para cada sistema o nodo de administración integrados. Los certificados de usuario de solución no deben incluir dirección IP, nombre de host ni dirección de correo electrónico. Cada certificado debe tener un asunto de certificado diferente.
   - De forma opcional, un certificado de usuario de la solución de máquina para las instancias de Platform Services Controller externas. Este certificado es distinto del certificado SSL de máquina para Platform Services Controller.

   Generalmente, el resultado es un archivo PEM para la cadena de confianza, junto con los certificados SSL firmados para cada sistema Platform Services Controller o nodo de administración.

2 Enumere los almacenes TRUSTED_ROOTS y SSL de máquina.

```
vecs-cli store list
```

a Asegúrese de que el certificado raíz actual y todos los certificados SSL de máquina estén firmados por VMCA.

b Anote el contenido de los campos Número de serie, Emisor y Nombre común de asunto.

c (opcional) Con un explorador web, abra una conexión HTTPS al nodo en el que se reubicará el certificado, compruebe la información del certificado y asegúrese de que esta coincida con la del certificado SSL de máquina.

3 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Publique el certificado raíz personalizado.

```
dir-cli trustedcert publish --cert <my_custom_root>
```

Si no especifica un nombre de usuario y una contraseña en la línea de comandos, el sistema se lo solicitará.

5 Reinicie todos los servicios.

```
service-control --start --all
```

Pasos siguientes

Se puede quitar el certificado raíz original de VMCA del almacén de certificados si así lo establece la directiva de la empresa. Si se hace eso, es necesario actualizar el certificado de vCenter Single Sign-On. Consulte Actualizar el certificado del servicio de token de seguridad.

Reemplazar certificados SSL de máquina por certificados personalizados

Después de recibir los certificados personalizados, puede reemplazar los certificados de cada máquina.

Cada máquina debe tener un certificado SSL de máquina para establecer una comunicación segura con otros servicios. En una implementación de varios nodos, debe ejecutar los comandos de generación de certificados SSL de máquina en cada nodo. Use el parámetro `--server` para apuntar a Platform Services Controller desde vCenter Server con Platform Services Controller externo.

Para poder empezar a reemplazar los certificados, debe tener la siguiente información:

- Contraseña de administrator@vsphere.local.
- Un certificado SSL de máquina personalizado y válido (archivo `.crt`).
- Una clave SSL de máquina personalizada y válida (archivo `.key`).
- Un certificado personalizado válido para la raíz (archivo `.crt`).
- Si ejecuta el comando en vCenter Server con Platform Services Controller externo en una implementación de varios nodos, la dirección IP de Platform Services Controller.

Requisitos previos

Seguramente recibió un certificado para cada máquina de la CA de la empresa o externa.

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Contiene los siguientes usos de claves: firma digital, cifrado de clave

Procedimiento

1 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

   Los nombres de servicios en Windows no son los mismos que en vCenter Server Appliance.

   Nota Si el entorno utiliza una instancia externa de Platform Services Controller, no es necesario detener e iniciar VMware Directory Service (vmdird) ni VMware Certificate Authority (vmcad) en el nodo de vCenter Server. Estos servicios se ejecutan en Platform Services Controller.

   Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

   vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

2 Inicie sesión en cada nodo y agregue a VECS los certificados de máquina nuevos obtenidos de la CA.

   Todas las máquinas necesitan el certificado nuevo en el almacén de certificados local para comunicarse mediante SSL.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-
path>
--key <key-file-path>
```

3 Reinicie todos los servicios.

```
service-control --start --all
```

Ejemplo: Reemplazar certificados SSL de máquina por certificados personalizados

En este ejemplo se muestra la manera en la que se debe reemplazar el certificado SSL de máquina por un certificado personalizado en una instalación de Windows. Puede reemplazar el certificado SSL de máquina en cada nodo del mismo modo.

1 Primero, elimine el certificado existente en VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

2 A continuación, agregue el certificado de reemplazo.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-w1-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

Reemplazar los certificados de usuarios de soluciones con certificados personalizados

Después de reemplazar los certificados SSL de máquina, puede reemplazar los certificados de usuarios de solución firmados por VMCA con certificados externas o empresariales.

Muchos clientes de VMware no reemplazan los certificados de usuario de las soluciones. Reemplazan solo los certificados SSL de los equipos con certificados personalizados. Este enfoque híbrido satisface los requisitos de sus equipos de seguridad.

- Los certificados se sientan detrás de un proxy, o bien son certificados personalizados.
- No se utilizan CA intermedias.

Los usuarios de soluciones usan los certificados únicamente para autenticarse en vCenter Single Sign-On. Si el certificado es válido, vCenter Single Sign-On asigna un token SAML al usuario de solución. Este usa el token SAML para autenticarse en otros componentes de vCenter.

Debe reemplazar el certificado de usuario de solución de la máquina en cada nodo de administración y en cada nodo de Platform Services Controller. Debe reemplazar los certificados de usuarios de solución solo en cada nodo de administración. Utilice el parámetro `--server` para apuntar a Platform Services Controller cuando ejecute comandos en un nodo de administración con una instancia externa de Platform Services Controller.

Nota Cuando se enumeran certificados de usuario de solución en implementaciones de gran tamaño, el resultado de `dir-cli list` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

Requisitos previos

- Tamaño de clave: 2.048 bits o más (formato codificado PEM)
- Formato CRT
- x509 versión 3
- SubjectAltName debe contener DNS Name=<machine_FQDN>.
- Cada certificado de usuario de solución debe tener un `Subject` diferente. Por ejemplo, considere incluir el nombre de usuario de solución (como vpxd) u otro identificador único.
- Contiene los siguientes usos de claves: firma digital, cifrado de clave

Procedimiento

1 Detenga todos los servicios e inicie los servicios que se ocupan de la creación, de la propagación y del almacenamiento de certificados.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

2 Busque el nombre de cada usuario de solución.

```
dir-cli service list
```

Puede usar el identificador único que se devuelve al reemplazar los certificados. La entrada y la salida deben verse de la siguiente manera.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Cuando enumera certificados de usuario de solución en implementaciones de varios nodos, el resultado de la lista de `dir-cli` incluye todos los usuarios de solución de todos los nodos. Ejecute `vmafd-cli get-machine-id --server-name localhost` para encontrar el identificador de máquina local para cada host. El nombre del usuario de solución incluye el identificador de máquina.

3 En cada usuario de solución, reemplace el certificado actual en VECS y, a continuación, en vmdir.

Debe agregar los certificados en ese orden.

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

Nota Los usuarios de solución no podrán autenticarse en vCenter Single Sign-On si no se reemplaza el certificado en vmdir.

4 Reinicie todos los servicios.

```
service-control --start --all
```

Reemplazar el certificado de VMware Directory Service en entornos de modo mixto

Durante la actualización, el entorno puede incluir temporalmente tanto la versión 5.5 de vCenter Single Sign-On como la versión 6.x de vCenter Single Sign-On. En ese caso, si reemplaza el certificado SSL del nodo en el que se está ejecutando el servicio de vCenter Single Sign-On, debe realizar pasos adicionales para reemplazar el certificado SSL de VMware Directory Service.

El vmdir utiliza el certificado SSL de VMware Directory Service para realizar negociaciones entre los nodos de Platform Services Controller que realizan la replicación de vCenter Single Sign-On.

Estos pasos no son necesarios para un entorno de modo mixto que incluya los nodos de vSphere 6.0 y vSphere 6.5. Estos pasos son necesarios solo si:

- El entorno incluye servicios tanto de vCenter Single Sign-On 5.5 como de vCenter Single Sign-On 6.x.
- Los servicios de vCenter Single Sign-On se configuran para replicar datos de vmdir.
- Planea reemplazar los certificados firmados por VMCA predeterminados por certificados personalizados del nodo en el que se ejecuta el servicio de vCenter Single Sign-On 6.x.

Nota Actualizar el entorno al completo antes de reiniciar los servicios es una práctica recomendada. Generalmente, el reemplazo del certificado de VMware Directory Service no se recomienda.

Procedimiento

1 En el nodo en el que se ejecuta el servicio de vCenter Single Sign-On 5.5, configure el entorno para que se reconozca el servicio de vCenter Single Sign-On 6.x.

   a Haga una copia de seguridad de todos los archivos `C:\ProgramData\VMware\CIS\cfg\vmdird`.

   b Haga una copia del archivo `vmdircert.pem` en el nodo 6.x y cámbiele el nombre por `<sso_node2.domain.com>.pem`, donde `<sso_node2.domain.com>` es el FQDN del nodo 6.x.

   c Copie el certificado con nombre nuevo en `C:\ProgramData\VMware\CIS\cfg\vmdird` para reemplazar el certificado de replicación existente.

2 Reinicie VMware Directory Service en todas las máquinas en las que reemplazó certificados.

   Puede reiniciar el servicio desde vSphere Client o utilizar el comando `service-control`.

Administrar servicios y certificados con comandos de CLI

4

Un conjunto de CLI permite administrar VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store) y VMware Directory Service (vmdir). La utilidad vSphere Certificate Manager también admite muchas tareas relacionadas, pero las CLI son necesarias para la administración manual de certificados y para administrar otros servicios.

Normalmente, las herramientas de CLI se usan para administrar los certificados y los servicios asociados mediante SSH con el fin de conectarse al shell del dispositivo. Consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2100508 para obtener más información.

Reemplazar certificados de forma manual proporciona ejemplos de reemplazo de certificados mediante comandos de CLI.

Tabla 4-1. Herramientas de CLI para administrar certificados y servicios asociados

CLI	Descripción	Consulte
`certool`	Genere y administre certificados y claves. Parte de VMCAD, el servicio VMware Certificate Management.	Referencia de comandos de inicialización de certool
`vecs-cli`	Administre el contenido de las instancias de VMware Certificate Store. Parte de VMAFD.	Referencia de comandos vecs-cli
`dir-cli`	Cree y actualice los certificados en VMware Directory Service. Parte de VMAFD.	Referencia de comando dir-cli
`sso-config`	Algunos parámetros de configuración de vCenter Single Sign-On. En la mayoría de los casos, se usa vSphere Web Client o vSphere Client. Use este comando para configurar la autenticación de dos factores.	Ayuda de línea de comandos. Descripción de la autenticación de dos factores de vCenter Server
`service-control`	Inicie o detenga los servicios (por ejemplo, como parte de un flujo de trabajo de reemplazo de certificados).	Ejecute este comando para detener servicios antes de ejecutar otros comandos de CLI.

Ubicaciones de CLI

De forma predeterminada, las CLI se encuentran en las siguientes ubicaciones de cada nodo:

Windows

`C:\Archivos de programa\VMware\vCenter Server\vmafdd\vecs-cli.exe`

`C:\Archivos de programa\VMware\vCenter Server\vmafdd\dir-cli.exe`

`C:\Archivos de programa\VMware\vCenter Server\vmcad\certool.exe`

`C:\Archivos de programa\VMware\VCenter server\VMware Identity Services\sso-config`

RUTA_DE_INSTALACIÓN_DE_VCENTER`\bin\service-control`

Linux

`/usr/lib/vmware-vmafd/bin/vecs-cli`

`/usr/lib/vmware-vmafd/bin/dir-cli`

`/usr/lib/vmware-vmca/bin/certool`

`/opt/vmware/bin`

En Linux, el comando `service-control` no requiere que especifique la ruta de acceso.

Si ejecuta comandos desde un sistema vCenter Server con Platform Services Controller externo, puede especificar Platform Services Controller con el parámetro `--server`.

Este capítulo incluye los siguientes temas:

- Privilegios necesarios para ejecutar CLI
- Cambiar las opciones de configuración de certool
- Referencia de comandos de inicialización de certool
- Referencia de comandos de administración de certool
- Referencia de comandos vecs-cli
- Referencia de comando dir-cli

Privilegios necesarios para ejecutar CLI

Los privilegios necesarios dependen de la CLI que esté usando y del comando que quiera ejecutar. Por ejemplo, para la mayoría de las operaciones de administración de certificados, tiene que ser administrador para el dominio de vCenter Single Sign-On local (vsphere.local de manera predeterminada). Algunos comandos están disponibles para todos los usuarios.

dir-cli

Debe ser miembro de un grupo de administradores en el dominio local (vsphere.local de manera predeterminada) para ejecutar los comandos `dir-cli`. Si no especifica un nombre de usuario y una contraseña, se le pedirá la contraseña para el administrador del dominio de vCenter Single Sign-On local, administrator@vsphere.local de manera predeterminada.

vecs-cli

Inicialmente, solo el propietario del almacén y los usuarios con privilegios de acceso ilimitado tienen acceso a un almacén. Los usuarios de grupo de administradores en Windows y los usuarios raíz en Linux tienen privilegios de acceso ilimitado.

Los almacenes MACHINE_SSL_CERT y TRUSTED_ROOTS son almacenes especiales. Solo el usuario raíz o el usuario administrador (según el tipo de instalación), tienen acceso total.

certool

La mayoría de los comandos `certool` requieren que el usuario esté en el grupo de administradores. Todos los usuarios pueden ejecutar los siguientes comandos.

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

Cambiar las opciones de configuración de certool

Al ejecutar `certool --gencert` u otros comandos específicos de inicialización o administración de certificados, el comando lee todos los valores de un archivo de configuración. Puede editar el archivo existente, anular el archivo de configuración predeterminado con la opción `--config=<file name>` o anular los diferentes valores en la línea de comandos.

El archivo de configuración, `certool.cfg`, se encuentra en la siguiente ubicación de forma predeterminada.

Sistema operativo	Ubicación
Linux	`/usr/lib/vmware-vmca/share/config/`
Windows	`C:\Archivos de programa\VMware\vCenter Server\vmcad\`

El archivo tiene varios campos con los siguientes valores predeterminados:

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

Puede cambiar los valores especificando un archivo modificado en la línea de comandos o anulando valores individuales en la línea de comandos, de la siguiente manera.

- Cree una copia del archivo de configuración y edite el archivo. Use la opción de línea de comandos `--config` para especificar el archivo. Especifique la ruta completa para evitar problemas con el nombre de la ruta.
-
  ```
  certool --gencert --config C:\Temp\myconfig.cfg
  ```
- Anule los valores individuales en la línea de comandos. Por ejemplo, para anular la localidad, ejecute el siguiente comando:

  ```
  certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

Especifique `--Name` para reemplazar el campo Nombre común del nombre de asunto del certificado.

- Para los certificados de usuarios de solución, el nombre es <sol_user name>@<domain> por convención, pero puede cambiarlo si se utiliza una convención diferente en el entorno.
- Para los certificados SSL de máquina, se utiliza el FQDN de la máquina.

  VMCA permite solo un DNSName (en el campo `Hostname`) y ninguna otra opción de alias. Si es el usuario quien especifica la dirección IP, esta también se almacena en SubAltName.

Use el parámetro `--Hostname` para especificar el DNSName de SubAltName del certificado.

Referencia de comandos de inicialización de certool

Los comandos de inicialización de `certool` permiten generar solicitudes de firma de certificados, ver y generar certificados y claves firmadas por VMCA, importar certificados raíz y realizar otras operaciones de administración de certificados.

En muchos casos, se puede pasar un archivo de configuración a un comando `certool`. Consulte Cambiar las opciones de configuración de certool. Consulte Reemplazar certificados firmados por VMCA existentes por certificados firmados por VMCA nuevos para ver algunos ejemplos de uso. La ayuda de la línea de comandos proporciona detalles sobre las opciones.

certool --initcsr

Genera una solicitud de firma de certificados (CSR). El comando genera un archivo PKCS10 y una clave privada.

Opción	Descripción
`--gencsr`	Se necesita para generar las CSR.
`--privkey <key_file>`	Nombre del archivo de clave privada.
`--pubkey <key_file>`	Nombre del archivo de clave pública.
`--csrfile <csr_file>`	Nombre del archivo de CSR que se enviará al proveedor de la entidad de certificación.
`--config <config_file>`	Nombre opcional del archivo de configuración. El valor predeterminado es `certool.cfg`.

Ejemplo:

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

Crea un certificado autofirmado y aprovisiona el servidor de VMCA con una entidad de certificación raíz autofirmada. Esta opción es una de las formas más simples de aprovisionar el servidor de VMCA. Otra opción es aprovisionar el servidor VMCA con un certificado raíz externo de modo que VMCA sea una entidad de certificación intermedia. Consulte Utilizar VMCA como entidad de certificación intermedia.

Este comando genera un certificado con la fecha establecida tres días antes para evitar conflictos entre las zonas horarias.

Opción	Descripción
`--selfca`	Se necesita para generar un certificado autofirmado.
`--predate <number_of_minutes>`	Permite establecer el campo No válido hasta del certificado raíz en la cantidad de minutos determinada antes de la hora actual. Esta opción puede resultar útil para dar cuenta de posibles problemas con las zonas horarias. El valor máximo es tres días.
`--config <config_file>`	Nombre opcional del archivo de configuración. El valor predeterminado es `certool.cfg`.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

Importa un certificado raíz. Agrega el certificado especificado y la clave privada a VMCA. VMCA usa siempre el certificado raíz más reciente para la firma, pero pueden quedar otros certificados raíz de confianza hasta que los elimina manualmente. Esto significa que el usuario puede actualizar la infraestructura un paso a la vez y, por último, eliminar los certificados que ya no use.

Opción	Descripción
`--rootca`	Se necesita para importar una entidad de certificación raíz.
`--cert <certfile>`	Nombre del archivo de certificado.
`--privkey <key_file>`	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

Devuelve el nombre de dominio predeterminado que usa vmdir.

Opción	Descripción
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
`--port <port_num>`	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --getdc
```

certool --waitVMDIR

Espere a que VMware Directory Service se ejecute o a que se cumpla el tiempo de espera especificado por `--wait`. Use esta opción, junto con otras opciones, para programar determinadas tareas, como obtener el nombre de dominio predeterminado.

Opción	Descripción
--wait	Cantidad opcional de minutos para esperar. El valor predeterminado es 3.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
--port <port_num>	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

Espere a que el servicio VMCA se ejecute o a que se cumpla el tiempo de espera especificado. Use esta opción, junto con otras opciones, para programar determinadas tareas, como generar un certificado.

Opción	Descripción
--wait	Cantidad opcional de minutos para esperar. El valor predeterminado es 3.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.
--port <port_num>	Número de puerto opcional. El valor predeterminado es el puerto 389.

Ejemplo:

```
certool --waitVMCA --selfca
```

certool --publish-roots

Fuerza la actualización de certificados raíz. Este comando requiere privilegios administrativos.

Opción	Descripción
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --publish-roots
```

Referencia de comandos de administración de certool

Los comandos de administración certool permiten ver, generar y revocar certificados, y ver información sobre ellos.

certool --genkey

Genera un par de claves privada y pública. Estos archivos se pueden utilizar para generar un certificado firmado por VMCA.

Opción	Descripción
--genkey	Se requiere para generar una clave privada y pública.
--privkey <keyfile>	Nombre del archivo de clave privada.
--pubkey <keyfile>	Nombre del archivo de clave pública.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

Genera un certificado desde el servidor de VMCA. Este comando utiliza la información de certool.cfg o del archivo de configuración especificado. Puede usar el certificado para aprovisionar certificados de máquinas o certificados de usuarios de solución.

Opción	Descripción
--gencert	Se requiere para generar un certificado.
--cert <certfile>	Nombre del archivo de certificado. Este archivo debe estar en el formato codificado PEM.
--privkey <keyfile>	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
--config <config_file>	Nombre opcional del archivo de configuración. El valor predeterminado es certool.cfg.
--server <server>	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

Imprime un certificado actual de la entidad de certificación raíz en formato de lenguaje natural. Si ejecuta este comando desde un nodo de administración, utilice el nombre de máquina del nodo de Platform Services Controller para recuperar la entidad de certificación raíz. Esta salida no se puede utilizar como certificado porque está cambiada a lenguaje natural.

Opción	Descripción
`--getrootca`	Se requiere para imprimir el certificado raíz.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --getrootca --server=remoteserver
```

certool --viewcert

Imprime todos los campos de un certificado en formato de lenguaje natural.

Opción	Descripción
`--viewcert`	Se requiere para ver un certificado.
`--cert <certfile>`	Nombre opcional del archivo de configuración. El valor predeterminado es `certool.cfg`.

Ejemplo:

```
certool --viewcert --cert=<filename>
```

certool --enumcert

Enumera todos los certificados que conoce el servidor de VMCA. La opción `filter` (filtrar) permite enumerar todos los certificados o solo los certificados revocados, activos o caducados.

Opción	Descripción
`--enumcert`	Se requiere para enumerar todos los certificados.
`--filter [all | active]`	Filtro requerido. Especifique todos o los que están activos. Las opciones revocadas o caducadas no se admiten en este momento.

Ejemplo:

```
certool --enumcert --filter=active
```

certool --status

Envía un certificado especificado al servidor de VMCA para comprobar si está revocado. Se muestra `Certificado: REVOCADO` si se revoca el certificado; de lo contrario, `Certificado: ACTIVO`.

Opción	Descripción
`--status`	Se requiere para comprobar el estado de un certificado.
`--cert <certfile>`	Nombre opcional del archivo de configuración. El valor predeterminado es `certool.cfg`.
`--server <server>`	Nombre opcional del servidor de VMCA. El comando usa el nombre localhost como valor predeterminado.

Ejemplo:

```
certool --status --cert=<filename>
```

certool --genselfcacert

Genera un certificado autofirmado a partir de los valores del archivo de configuración. Este comando genera un certificado con la fecha establecida tres días antes para evitar conflictos entre las zonas horarias.

Opción	Descripción
`--genselfcacert`	Se necesita para generar un certificado autofirmado.
`--outcert <cert_file>`	Nombre del archivo de certificado. Este archivo debe estar en el formato codificado PEM.
`--outprivkey <key_file>`	Nombre del archivo de clave privada. Este archivo debe estar en el formato codificado PEM.
`--config <config_file>`	Nombre opcional del archivo de configuración. El valor predeterminado es `certool.cfg`.

Ejemplo:

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

Referencia de comandos vecs-cli

El conjunto de comandos `vecs-cli` permite administrar las instancias de VMware Certificate Store (VECS). Utilice estos comandos junto con `dir-cli` y `certool` para administrar la infraestructura de certificados y demás servicios de Platform Services Controller.

vecs-cli store create

Crea un almacén de certificados.

Opción	Descripción
--name <name>	Nombre del almacén de certificados.
--server <server-name>	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
--upn <user-name>	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por --server <server-name> . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

Ejemplo:

```
vecs-cli store create --name <store>
```

vecs-cli store delete

Elimina un almacén de certificados. Puede eliminar los almacenes del sistema MACHINE_SSL_CERT, TRUSTED_ROOTS y TRUSTED_ROOT_CRLS. Los usuarios con privilegios exigidos pueden eliminar los almacenes de usuarios de solución.

Opción	Descripción
--name <name>	Nombre del almacén de certificados que se va a eliminar.
--server <server-name>	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
--upn <user-name>	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por --server <server-name> . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

Ejemplo:

```
vecs-cli store delete --name <store>
```

vecs-cli store list

Enumera los almacenes de certificados.

Opción	Descripción
--server <server-name>	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
--upn <user-name>	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por --server <server-name> . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

VECS incluye los siguientes almacenes.

Tabla 4-2. Almacenes en VECS

Almacén	Descripción
Almacén SSL de máquina (MACHINE_SSL_CERT)	■ El servicio de proxy inverso lo utiliza en cada nodo de vSphere. ■ VMware Directory Service (vmdir) lo utiliza en implementaciones integradas y en cada nodo de Platform Services Controller. Todos los servicios de vSphere 6.0 y versiones posteriores se comunican mediante un proxy inverso que utiliza el certificado SSL de equipo. Por razones de compatibilidad con versiones anteriores, los servicios de la versión 5.x todavía utilizan puertos específicos. Como resultado, algunos servicios como vpxd todavía tienen su propio puerto abierto.
Almacén raíz de confianza (TRUSTED_ROOTS)	Contiene todos los certificados raíz de confianza.

Tabla 4-2. Almacenes en VECS (continuación)

Almacén	Descripción
Almacenes de usuarios de solución ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient`	VECS incluye un almacén para cada usuario de solución. El asunto de cada certificado de usuario de solución debe ser único, por ejemplo, el certificado de máquina no puede tener el mismo asunto que el certificado de vpxd. Los certificados de usuarios de solución se utilizan para la autenticación con vCenter Single Sign-On. vCenter Single Sign-On comprueba que el certificado sea válido, pero no comprueba otros atributos del certificado. En una implementación integrada, todos los certificados de usuarios de solución están en el mismo sistema. Los siguientes almacenes de certificados de usuarios de solución se incluyen en VECS en cada nodo de administración y en cada implementación integrada: ■ `machine`: lo utilizan el servidor de licencias y el servicio de registro. **Nota** El certificado de usuario de solución de la máquina no tiene relación alguna con el certificado SSL de máquina. El certificado de usuario de solución de la máquina se utiliza para el intercambio de tokens SAML, mientras que el certificado SSL de máquina se utiliza para las conexiones SSL seguras de una máquina. ■ `vpxd`: almacén de daemon del servicio vCenter (vpxd) de los nodos de administración y las implementaciones integradas. vpxd utiliza el certificado de usuario de solución que está en este almacén para autenticarse en vCenter Single Sign-On. ■ `vpxd-extension`: almacén de extensiones de vCenter. Incluye el servicio de Auto Deploy, el servicio de inventario u otros servicios que no forman parte de otros usuarios de solución. ■ `vsphere-webclient`: almacén de vSphere Web Client. También incluye algunos servicios adicionales como el servicio de gráficos de rendimiento. Cada nodo de Platform Services Controller incluye un certificado `machine`.

Tabla 4-2. Almacenes en VECS (continuación)

Almacén	Descripción
Almacén de copias de seguridad de la utilidad vSphere Certificate Manager (BACKUP_STORE)	VMCA (VMware Certificate Manager) lo utiliza para admitir la reversión de certificados. Solo el estado más reciente se almacena como copia de seguridad; no se puede volver más de un paso.
Otros almacenes	Las soluciones pueden agregar otros almacenes. Por ejemplo, la solución Virtual Volumes agrega un almacén SMS. No modifique los certificados de estos almacenes a menos que así se indique en la documentación de VMware o en un artículo de la base de conocimientos de VMware. **Nota** La eliminación del almacén TRUSTED_ROOTS_CRLS puede dañar la infraestructura de certificado. No elimine ni modifique el almacén TRUSTED_ROOTS_CRLS.

Ejemplo:

```
vecs-cli store list
```

vecs-cli store permissions

Otorga o revoca permisos en el almacén. Utilice la opción `--grant` o `--revoke`.

El propietario de almacén puede realizar todas las operaciones, incluso otorgar y revocar permisos. El administrador del dominio local de vCenter Single Sign-On, administrator@vsphere.local de manera predeterminada, tiene todos los privilegios en todos los almacenes, incluso otorgar y revocar permisos.

Se puede utilizar `vecs-cli get-permissions --name <store-name>` para recuperar la configuración actual del almacén.

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td>--name <name></td><td>Nombre del almacén de certificados.</td></tr>
<tr><td>--user <username></td><td>Nombre único del usuario al que se otorgan permisos.</td></tr>
<tr><td>--grant [read|write]</td><td>Permiso que se va a otorgar, ya sea de lectura o de escritura.</td></tr>
<tr><td>--revoke [read|write]</td><td>Permiso que se va a revocar, ya sea de lectura o de escritura. No es compatible en este momento.</td></tr>
</table>

vecs-cli store get-permissions

Recupera la configuración de permiso actual para el almacén.

Opción	Descripción
`--name <name>`	Nombre del almacén de certificados.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry create

Crea una entrada en VECS. Utilice este comando para agregar una clave privada o un certificado a un almacén.

Opción	Descripción
`--store <NameOfStore>`	Nombre del almacén de certificados.
`--alias <Alias>`	Alias opcional del certificado. Esta opción se ignora para el almacén raíz de confianza.
`--cert <certificate_file_path>`	Ruta de acceso completa del archivo de certificado.
`--key <key-file-path>`	Ruta de acceso completa de la clave que corresponde al certificado. Opcional.
`--password <password>`	Contraseña opcional para cifrar la clave privada.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry list

Enumera todas las entradas en un almacén especificado.

Opción	Descripción
`--store <NameOfStore>`	Nombre del almacén de certificados.

vecs-cli entry getcert

Recupera un certificado de VECS. Es posible enviar el certificado en un archivo de salida o mostrarlo como texto en lenguaje natural.

Opción	Descripción
`--store <NameOfStore>`	Nombre del almacén de certificados.
`--alias <Alias>`	Alias del certificado.
`--output <output_file_path>`	Archivo donde se escribe el certificado.
`--text`	Muestra una versión del certificado en lenguaje natural.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry getkey

Recupera una clave almacenada en VECS. Es posible enviar la clave en un archivo de salida o mostrarla como texto en lenguaje natural.

Opción	Descripción
`--store <NameOfStore>`	Nombre del almacén de certificados.
`--alias <Alias>`	Alias de la clave.
`--output <output_file_path>`	Archivo de salida donde se escribe la clave.
`--text`	Muestra una versión de la clave en lenguaje natural.
`--server <server-name>`	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
`--upn <user-name>`	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por `--server <server-name>` . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

vecs-cli entry delete

Elimina una entrada de un almacén de certificados. Si se elimina una entrada en VECS, esta se quita de forma permanente de VECS. La única excepción es el certificado raíz actual. VECS sondea vmdir en busca de un certificado raíz.

Opción	Descripción
--store <NameOfStore>	Nombre del almacén de certificados.
--alias <Alias>	Alias de la entrada que se desea eliminar.
--server <server-name>	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
--upn <user-name>	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por --server <server-name> . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.
-y	Suprime la solicitud de confirmación. Para usuarios avanzados solamente.

vecs-cli force-refresh

Fuerza una actualización de VECS. De forma predeterminada, VECS sondea vmdir cada 5 minutos en busca de archivos de certificado raíz nuevos. Utilice este comando para realizar una actualización inmediata de VECS desde vmdir.

Opción	Descripción
--server <server-name>	Se utiliza para especificar un nombre de servidor si el usuario se conecta a una instancia de VECS remota.
--upn <user-name>	Nombre principal del usuario que se utiliza para iniciar sesión en la instancia de servidor especificada por --server <server-name> . Cuando crea un almacén, se crea en el contexto del usuario actual. En consecuencia, el propietario del almacén es el contexto del usuario actual y no siempre el usuario raíz.

Referencia de comando dir-cli

La utilidad `dir-cli` admite la creación y actualización de usuarios de solución, administración de cuentas y administración de certificados y contraseñas en VMware Directory Service (vmdir). También puede usar `dir-cli` para administrar y consultar el nivel funcional de dominio de las instancias de Platform Services Controller.

dir-cli nodes list

Enumera todos los sistemas vCenter Server para la instancia de Platform Services Controller especificada.

Opción	Descripción
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.
--server <psc_ip_or_fqdn>	Utilice esta opción si no desea usar como destino el Platform Services Controller afín. Especifique la dirección IP o el FQDN de Platform Services Controller.

dir-cli computer password-reset

Permite restablecer la contraseña de la cuenta de máquina en el dominio. Es una opción útil cuando hay que restaurar una instancia de Platform Services Controller.

Opción	Descripción
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.
--live-dc-hostname <server name>	Nombre actual de la instancia de Platform Services Controller.

dir-cli service create

Crea un usuario de solución. Se usa sobre todo en soluciones externas.

Opción	Descripción
--name <name>	Nombre del usuario de solución que se va a crear
--cert <cert file>	Ruta de acceso al archivo de certificado. Puede ser un certificado firmado por VMCA o un certificado externo.
--ssogroups <comma-separated-groupnames>	Incluye al usuario de la solución como miembro de los grupos especificados.
--wstrustrole <ActAsUser>	Incluye al usuario de la solución como miembro del grupo integrado de administradores o usuarios. En otras palabras, determina si el usuario de la solución tiene privilegios administrativos.
--ssoadminrole <Administrator/User>	Incluye al usuario de la solución como miembro del grupo ActAsUser. La función ActAsUser permite a los usuarios actuar en nombre de otros usuarios.

Opción	Descripción
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli service list

Enumera a los usuarios de solución que conoce `dir-cli`.

Opción	Descripción
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli service delete

Elimina un usuario de solución en vmdir. Cuando se elimina el usuario de solución, todos los servicios asociados dejan de estar disponibles en los nodos de administración que usan esta instancia de vmdir.

Opción	Descripción
`--name`	Nombre del usuario de solución que se va a eliminar.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli service update

Actualiza el certificado de un usuario de solución especificado, es decir, de una recopilación de servicios. Después de ejecutar este comando, VECS aplica el cambio transcurridos 5 minutos; o bien también se puede usar `vecs-cli force-refresh` para forzar la actualización.

Opción	Descripción
`--name <name>`	Nombre del usuario de solución que se va a actualizar.
`--cert <cert_file>`	Nombre del certificado que se va a asignar al servicio.

Opción	Descripción
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user create

Crea un usuario regular en vmdir. Este comando puede usarse para usuarios humanos que se autentican en vCenter Single Sign-On con un nombre de usuario y una contraseña. Use este comando únicamente durante la creación de prototipos.

Opción	Descripción
--account <name>	Nombre del usuario de vCenter Single Sign-On que se va a crear.
--user-password <password>	Contraseña inicial del usuario.
--first-name <name>	Nombre de pila del usuario.
--last-name <name>	Apellido del usuario.
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user modify

Modifica el usuario especificado dentro de vmdir.

Opción	Descripción
--account <name>	Nombre del usuario de vCenter Single Sign-On que se va a modificar.
--password-never-expires	Esta opción se establece en true si va a crear una cuenta de usuario para tareas automatizadas que deben autenticarse en Platform Services Controller y desea asegurarse de que no se detenga la ejecución de las tareas por caducidad de contraseñas. Utilice con atención esta opción.
--password-expires	Esta opción se establece en true si desea revertir la opción --password-never-expires.

Opción	Descripción
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user delete

Elimina el usuario especificado en vmdir.

Opción	Descripción
`--account <name>`	Nombre del usuario de vCenter Single Sign-On que se va a eliminar.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli user find-by-name

Busca usuarios por nombre en vmdir. La información que devuelve este comando depende de lo que se especifique en la opción `--level`.

Opción	Descripción
`--account <name>`	Nombre del usuario de vCenter Single Sign-On que se va a eliminar.
`--level <info level 0|1|2>`	Devuelve la siguiente información: ■ Nivel 0: cuenta y UPN ■ Nivel 1: información del nivel 0 + nombre y apellido ■ Nivel 2: nivel 0 + marca de cuenta deshabilitada, marca de cuenta bloqueada, marca de contraseña sin fecha de caducidad, marca de contraseña caducada y marca de caducidad de contraseña. El nivel predeterminado es 0.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli group modify

Agrega un usuario o un grupo a un grupo que ya existe.

Opción	Descripción
`--name <name>`	Nombre del grupo en vmdir.
`--add <user_or_group_name>`	Nombre del usuario o el grupo que se va a agregar.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli group list

Enumera un grupo de vmdir específico.

Opción	Descripción
`--name <name>`	Nombre opcional del grupo en vmdir. Esta opción permite comprobar si existe un grupo específico.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli ssogroup create

Crea un grupo en el dominio local (vsphere.local de forma predeterminada).

Use este comando si desea crear grupos para administrar los permisos del usuario en el dominio de vCenter Single Sign-On. Por ejemplo, si crea un grupo y luego lo agrega al grupo Administradores del dominio de vCenter Single Sign-On, todos los usuarios que agregue al grupo tendrán permisos de administrador en el dominio.

También es posible otorgar permisos para los objetos de inventario de vCenter a los grupos del dominio de vCenter Single Sign-On. Consulte la documentación de *Seguridad de vSphere*.

Opción	Descripción
`--name <name>`	Nombre del grupo en vmdir. La longitud máxima es de 487 caracteres.
`--description <description>`	Descripción opcional para el grupo.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli trustedcert publish

Publica un certificado raíz de confianza en vmdir.

Opción	Descripción
--cert <file>	Ruta de acceso al archivo de certificado.
--crl <file>	Esta opción no es compatible con VMCA.
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.
--chain	Especifique esta opción si va a publicar un certificado encadenado. No se requiere ningún valor de opción.

dir-cli trustedcert publish

Publica un certificado raíz de confianza en vmdir.

Opción	Descripción
--cert <file>	Ruta de acceso al archivo de certificado.
--crl <file>	Esta opción no es compatible con VMCA.
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.
--chain	Especifique esta opción si va a publicar un certificado encadenado. No se requiere ningún valor de opción.

dir-cli trustedcert unpublish

Anula la publicación de un certificado raíz de confianza que actualmente está en vmdir. Utilice este comando, por ejemplo, si agregó un certificado raíz diferente a vmdir que es ahora el certificado raíz de todos los otros certificados del entorno. La anulación de la publicación de los certificados que ya no se utilizan forma parte del fortalecimiento del entorno.

Opción	Descripción
--cert-file <file>	Ruta de acceso al archivo de certificado cuya publicación se va a anular.
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli trustedcert list

Enumera todos los certificados raíz de confianza y sus correspondientes identificadores Los identificadores de los certificados son necesarios para recuperar un certificado con dir-cli trustedcert get.

Opción	Descripción
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli trustedcert get

Recupera un certificado raíz de confianza desde vmdir y lo escribe en un archivo especificado.

Opción	Descripción
--id <cert_ID>	Identificador del certificado que se va a recuperar. El comando dir-cli trustedcert list muestra el identificador.
--outcert <path>	Ruta de acceso donde se escribe el archivo de certificado.
--outcrl <path>	Ruta de acceso donde se escribe el archivo CRL. No se encuentra en uso.
--login <admin_user_id>	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
--password <admin_password>	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli password create

Crea una contraseña aleatoria que cumple con los requisitos de contraseñas. Este comando puede ser utilizado por usuarios de solución externa.

Opción	Descripción
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli password reset

Permite que un administrador restablezca la contraseña de un usuario. Si usted es un usuario sin permisos de administrador y desea restablecer una contraseña, utilice el comando `dir-cli password change`.

Opción	Descripción
`--account`	Nombre de la cuenta a la que se le asignará una nueva contraseña.
`--new`	Nueva contraseña del usuario especificado.
`--login <admin_user_id>`	El administrador del dominio de vCenter Single Sign-On local (de manera predeterminada, administrator@vsphere.local).
`--password <admin_password>`	Contraseña del usuario administrador. Si no especifica la contraseña, se solicitará que lo haga.

dir-cli password change

Le permite a un usuario cambiar su contraseña. Es necesario ser el usuario propietario de la cuenta para poder hacer este cambio. Los administradores pueden utilizar el comando `dir-cli password reset` para restablecer cualquier contraseña.

Opción	Descripción
`--account`	Nombre de la cuenta.
`--current`	Contraseña actual del usuario propietario de la cuenta.
`--new`	Nueva contraseña del usuario propietario de la cuenta.

Solucionar problemas en Platform Services Controller

5

Los siguientes temas ofrecen un punto de partida para la solución de problemas en Platform Services Controller. Para más información, busque en este centro de documentación y en la base de conocimientos de VMware.

Este capítulo incluye los siguientes temas:

- Determinar la causa de un error de Lookup Service
- No se puede iniciar sesión con la autenticación del dominio de Active Directory
- Se produce un error en el inicio de sesión en vCenter Server porque la cuenta de usuario está bloqueada
- La replicación de VMware Directory Service puede tardar mucho
- Exportar un paquete de soporte de Platform Services Controller
- Referencia a registros del servicio Platform Services Controller

Determinar la causa de un error de Lookup Service

La instalación de vCenter Single Sign-On muestra un error relacionado con vCenter Server, vSphere Client o vSphere Web Client.

Problema

Los programas de instalación de vCenter Server y Web Client muestran el error `Could not contact Lookup Service. Please check VM_ssoreg.log....`

Causa

Este problema tiene varias causas, como relojes no sincronizados en los equipos host, bloqueos de firewall y servicios que deben iniciarse.

Solución

1 Compruebe que los relojes de los equipos host que ejecutan vCenter Single Sign-On, vCenter Server y Web Client estén sincronizados.

2 Vea el archivo de registro específico que se encuentra en el mensaje de error.

   En el mensaje, la carpeta temporal del sistema hace referencia a `%TEMP%`.

3 En el archivo de registro, busque los siguientes mensajes.

El archivo de registro contiene una salida de todos los intentos de instalación. Busque el último mensaje que muestra `Initializing registration provider...`

Mensaje	Causa y solución
`java.net.ConnectException: Connection timed out: connect`	La dirección IP es incorrecta, hay un firewall bloqueando el acceso a vCenter Single Sign-On o vCenter Single Sign-On está sobrecargado. Asegúrese de que un firewall no esté bloqueando el puerto de vCenter Single Sign-On (de manera predeterminada es el 7444). Compruebe también que el equipo donde está instalado vCenter Single Sign-On tenga suficiente capacidad libre de CPU, RAM y E/S.
`java.net.ConnectException: Connection refused: connect`	La dirección IP o el FQDN son incorrectos y el servicio vCenter Single Sign-On no se inició o se inició en el último minuto. Compruebe que vCenter Single Sign-On funcione. Para ello, consulte el estado del servicio vCenter Single Sign-On (Windows) y el daemon vmware-sso (Linux). Reinicie el servicio. Si el reinicio no soluciona el problema, consulte la sección Recuperación de la guía *Solucionar problemas de vSphere*.
`Unexpected status code: 404. SSO Server failed during initialization`	Reinicie vCenter Single Sign-On. Si el reinicio no soluciona el problema, consulte la sección Recuperación de la guía *Solucionar problemas de vSphere*.
El error que se muestra en la interfaz de usuario comienza con `Could not connect to vCenter Single Sign-On`	También se observa el código de retorno `SslHandshakeFailed`. Este error indica que la dirección IP o el FQDN proporcionados que se resuelven en el host de vCenter Single Sign-On no era la dirección que se utilizó cuando se instaló vCenter Single Sign-On. En `%TEMP%\VM_ssoreg.log`, busque la línea que contiene el siguiente mensaje. `host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>` donde A era el FQDN que se introdujo durante la instalación de vCenter Single Sign-On, y B y C eran las alternativas permitidas generadas por el sistema. Corrija la configuración para utilizar el FQDN a la derecha del signo `!=` del archivo de registro. En la mayoría de los casos, utilice el FQDN que especificó durante la instalación de vCenter Single Sign-On. Si ninguna de las alternativas es posible en la configuración de la red, recupere la configuración de SSL de vCenter Single Sign-On.

No se puede iniciar sesión con la autenticación del dominio de Active Directory

Puede iniciar sesión en un componente de vCenter Server desde vSphere Client o desde vSphere Web Client. Se utiliza el nombre de usuario y la contraseña de Active Directory. Se produce un error en la autenticación.

Problema

Se agrega el origen de identidad de Active Directory a vCenter Single Sign-On, pero los usuarios no pueden iniciar sesión en vCenter Server.

Causa

Los usuarios utilizan su nombre de usuario y contraseña para iniciar sesión en el dominio predeterminado. Para los demás dominios, los usuarios deben incluir el nombre de dominio (usuario@dominio o DOMINIO\usuario).

Si está utilizando vCenter Server Appliance, es posible que se produzcan otros problemas.

Solución

En todas las implementaciones de vCenter Single Sign-On,se puede cambiar el origen de identidad predeterminado. Después de ese cambio, los usuarios pueden iniciar sesión en el origen de identidad predeterminado únicamente con el nombre de usuario y la contraseña.

Para configurar un origen de identidad para Autenticación de Windows integrado con un dominio secundario dentro del bosque de Active Directory, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/2070433. De forma predeterminada, la autenticación integrada de Windows utiliza el dominio raíz del bosque de Active Directory.

Si utiliza vCenter Server Appliance y el cambio del origen de identidad predeterminado no soluciona el problema, siga estos pasos adicionales de solución de problemas.

1 Sincronice los relojes entre vCenter Server Appliance y las controladoras de dominio de Active Directory.

2 Compruebe que cada controlador de dominio tenga un registro de puntero (pointer record, PTR) en el servicio DNS del dominio de Active Directory.

   Compruebe que la información del registro PTR para el controlador de dominio coincida con el nombre DNS del controlador. Al utilizar vCenter Server Appliance, ejecute los siguientes comandos para realizar la tarea:

   a Para enumerar los controladores de dominio, ejecute el siguiente comando:

   ```
   # dig SRV _ldap._tcp.my-ad.com
   ```

   Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

   ```
   ;; ANSWER SECTION:
   _ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
   ...
   ```

b Para cada controladora de dominio, compruebe la resolución de nombres en las direcciones IP (conocida como forward) y la resolución inversa mediante el comando siguiente:

```
# dig my-controller.my-ad.com
```

Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A controller IP address
...
```

```
# dig -x <controller IP address>
```

Las direcciones relevantes aparecen en la sección de respuestas, como en el ejemplo siguiente:

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

3 Si esto no soluciona el problema, quite vCenter Server Appliance del dominio de Active Directory y vuelva a asociar el dominio. Consulte la documentación de *Configuración de vCenter Server Appliance*.

4 Cierre todas las sesiones del explorador que estén conectadas a vCenter Server Appliance y reinicie los servicios.

```
/bin/service-control --restart --all
```

Se produce un error en el inicio de sesión en vCenter Server porque la cuenta de usuario está bloqueada

Al iniciar sesión en vCenter Server desde la página de inicio de sesión de vSphere Client o de vSphere Web Client, se muestra un error que indica que la cuenta está bloqueada.

Problema

Después de varios intentos con errores, no puede iniciar sesión en vSphere Client o vSphere Web Client mediante vCenter Single Sign-On. Aparece un mensaje que indica que la cuenta está bloqueada.

Causa

Se supera la cantidad máxima de intentos de inicio de sesión con errores.

Solución

- Si intentó iniciar sesión como usuario desde el dominio del sistema (vsphere.local de manera predeterminada), solicítele al administrador de vCenter Single Sign-On que desbloquee la cuenta. Si el bloqueo está configurado para caducar en la directiva de bloqueo, puede esperar hasta que la cuenta se desbloquee. Los administradores de vCenter Single Sign-On pueden usar comandos de CLI para desbloquear la cuenta.
- Si inicia sesión como usuario desde el dominio de Active Directory o de LDAP, solicítele al administrador de Active Directory o LDAP que desbloquee la cuenta.

La replicación de VMware Directory Service puede tardar mucho

Si el entorno incluye varias instancias de Platform Services Controller, y si una de las instancias de Platform Services Controller deja de estar disponible, el entorno continúa funcionando. Cuando Platform Services Controller vuelve a estar disponible, se suelen replicar los datos del usuario y demás información en un plazo de 60 segundos. Sin embargo, ante algunas circunstancias especiales, la replicación puede tardar mucho.

Problema

En ciertas situaciones, por ejemplo, cuando el entorno incluye varias instancias de Platform Services Controller en diferentes ubicaciones, y se realizan cambios significativos mientras una instancia de Platform Services Controller no está disponible, no se ve de inmediato la replicación en todas las instancias de VMware Directory Service. Por ejemplo, el usuario nuevo que se agregó a la instancia disponible de Platform Services Controller no se puede ver en la otra instancia hasta que la replicación está completa.

Causa

En condiciones de funcionamiento normal, los cambios que se realizan en la instancia de VMware Directory Service (vmdir) en una instancia de Platform Services Controller (nodo) aparecen en su partner de replicación directo en un plazo de 60 segundos. Según la topología de la replicación, es posible que los cambios realizados en un nodo deban propagarse por nodos intermedios antes de llegar a cada instancia de vmdir en cada nodo. La información que se replica incluye información del usuario, de certificados, de licencias para las máquinas virtuales creadas, clonadas o migradas con VMware vMotion, entre otras.

Cuando se rompe el vínculo de replicación, por ejemplo, debido a una interrupción de la red o porque un nodo dejó de estar disponible, los cambios en la federación no convergen. Una vez que se restaura el nodo no disponible, cada nodo intenta actualizarse con todos los cambios. Finalmente, todas las instancias de vmdir convergen en un estado coherente, pero puede llevar un tiempo alcanzar ese estado si se produjeron muchos cambios mientras un nodo no estaba disponible.

Solución

El entorno funciona con normalidad mientras se lleva a cabo la replicación. No intente resolver el problema a menos que persista durante más de una hora.

Exportar un paquete de soporte de Platform Services Controller

Es posible exportar un paquete de soporte con los archivos de registro para los servicios de Platform Services Controller. Después de la exportación, puede explorar los registros localmente o enviar el paquete al soporte técnico de VMware.

Requisitos previos

Compruebe que el dispositivo virtual de Platform Services Controller esté implementado y ejecutándose correctamente.

Procedimiento

1 Desde un explorador web, conéctese a la interfaz de administración de Platform Services Controller en https://*platform_services_controller_ip*:5480.

2 Inicie sesión como usuario raíz para el dispositivo virtual.

3 En el menú **Acciones**, seleccione **Crear paquete de soporte**.

4 El paquete de soporte se guarda en la máquina local, a menos que la configuración del explorador evite una descarga inmediata.

Referencia a registros del servicio Platform Services Controller

Los servicios de Platform Services Controller usan syslog para el registro. Puede examinar los archivos de registro para determinar cuáles son las causas de los errores.

La siguiente tabla muestra la ubicación de los registros de la vCenter Server Appliance. En las implementaciones de Windows, la mayoría de los registros se encuentran en el directorio `C:\ProgramData\VMware\vCenterServer\logs`.

Tabla 5-1. Registros de servicio

Servicio	Descripción
VMware Directory Service	De manera predeterminada, el registro de vmdir va a /var/log/messages o /var/log/vmware/vmdird/. Para los problemas en el tiempo de implementación, /var/log/vmware/vmdir/vmafdvmdirclient.log también puede contener datos útiles sobre solución de problemas.
VMware Single Sign-On	El registro de vCenter Single Sign-On va a /var/log/vmware/sso/.
VMware Certificate Authority (VMCA)	El registro del servicio VMCA se encuentra en /var/log/vmware/vmcad/vmcad-syslog.log.
Almacén de certificados de endpoints de VMware (VECS)	El registro del servicio VECS se encuentra en /var/log/vmware/vmafdd/vmafdd-syslog.log.
VMware Lookup Service	El registro del servicio de búsqueda se encuentra en /var/log/vmware/sso/lookupServer.log.